

EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA EN EL USO DE  
DISPOSITIVOS MÓVILES EN LA COMUNIDAD ESTUDIANTIL DE LA INSTITUCIÓN  
EDUCATIVA CATUMARE DE LA CIUDAD DE VILLAVICENCIO PARA LOS GRADOS DE  
MEDIA BÁSICA 9, 10 Y 11.

BELKYN BAWER RODRÍGUEZ LEÓN



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
VILLAVICENCIO META,  
MAYO DE 2019

EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA EN EL USO DE  
DISPOSITIVOS MÓVILES EN LA COMUNIDAD ESTUDIANTIL DE LA INSTITUCIÓN  
EDUCATIVA CATUMARE DE LA CIUDAD DE VILLAVICENCIO PARA LOS GRADOS DE  
MEDIA BÁSICA 9, 10 Y 11.

BELKYN BAWER RODRÍGUEZ LEÓN

Trabajo de grado presentado como requisito para optar al título de Especialista En  
Seguridad Informática

Alexander Larrahondo Nuez  
Director de Proyecto

Christian Angulo Rivera  
MBA, Esp. En Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
VILLAVICENCIO META,  
MAYO DE 2019

Nota de aceptación

---

---

---

---

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

Villavicencio Meta, Julio 2019.

## DEDICATORIA

A Dios, por permitirme alcanzar esta nueva etapa de mi proceso de formación profesional.

A mi esposa, por el apoyo incondicional y paciencia que han tenido y demostrado por mí en este proceso.

A mi hija, por ser parte de mi inspiración para avanzar en la vida.

## CONTENIDO

	Pág.
INTRODUCCIÓN .....	34
1. PLANTEAMIENTO DEL PROBLEMA .....	35
1.1. DESCRIPCIÓN DEL PROBLEMA.....	35
2. FORMULACIÓN DEL PROBLEMA .....	37
3. JUSTIFICACIÓN .....	38
4. OBJETIVOS .....	39
4.1. OBJETIVO GENERAL.....	39
4.2. OBJETIVOS ESPECÍFICOS .....	39
5. MARCO TEÓRICO.....	40
5.1. MARCO REFERENCIAL .....	40
5.2. MARCO CONCEPTUAL.....	42
5.3. MARCO LEGAL .....	44
5.4. ESTADO DEL ARTE .....	45
6. DISEÑO METODOLÓGICO .....	47
6.1. MÉTODO - ESTRUCTURA DE LA UNIDAD DE ANÁLISIS .....	47
6.1.1. Tipo de estudio. ....	47
6.1.2. Tipo de investigación .....	47
6.1.3. Plan de trabajo. ....	65
6.2. DEFINICIÓN DE HIPÓTESIS.....	66
6.3. VARIABLES .....	66
6.3.1. Independientes. ....	66
6.3.2. Dependientes. ....	66
6.4. UNIVERSO, POBLACIÓN Y MUESTRA .....	67
6.5. INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN .....	67
6.5.1. Presentación.....	67
6.5.2. Observación en campo.....	68
6.5.3. Encuestas.....	68
6.6. FASES DE LA METODOLOGÍA.....	70
6.6.1. Preliminar. ....	70
6.6.2. Introductoria.....	70

6.6.3.	Desarrollo .....	70
6.6.4.	Finales.....	71
7.	LA INSTITUCIÓN .....	72
8.	CRONOGRAMA DE ACTIVIDADES .....	74
9.	DESARROLLO DE LA METODOLOGÍA.....	75
9.1.	PRELIMINAR .....	75
9.2.	INTRODUCTORIA .....	75
9.3.	DESARROLLO .....	76
9.4.	FINALES .....	76
10.	RESULTADOS OBTENIDOS DE LA ENCUESTA.....	77
10.1.	TABULACIÓN PRIMERA ENCUESTA.....	79
10.2.	TABULACIÓN SEGUNDA ENCUESTA .....	90
11.	CONCLUSIONES.....	93
12.	RECOMENDACIONES .....	95
13.	DIFICULTADES .....	96
14.	BIBLIOGRAFÍA .....	97
	ANEXOS .....	98

## LISTA DE TABLAS

	Pág.
Tabla 1. Formato encuesta.....	69
Tabla 2. Distribución de cursos .....	73
Tabla 3. Cronograma de actividades .....	74
Tabla 4. Programación de actividades fase de desarrollo .....	75
Tabla 5. Tabulación primera encuesta aplicada .....	79
Tabla 6. Tabulación final encuesta aplicada.....	90

## LISTA DE FIGURAS

	Pág.
Figura 1. Distribución de la población objetivo .....	67
Figura 2. Porcentaje de distribución de la muestra de acuerdo al sexo.....	77
Figura 3. Distribución de la muestra de acuerdo a la edad.....	78
Figura 4. Distribución de la muestra por estrato socio-económico .....	78



## RESUMEN

La siguiente propuesta de trabajo de grado, busca evaluar a un grupo de estudiantes pertenecientes a la Institución Educativa Catumare en la ciudad de Villavicencio, sobre las medidas y el nivel de seguridad que implementan al hacer uso de sus celulares Smartphone, relacionadas con el uso de sus redes sociales, manejo de su información personal, así como de terceros.

El objetivo del proyecto planteado se alinea con el lema de la Institución Educativa “*Comprometidos con el desarrollo de la calidad Humana*”, y la Misión Institucional la cual consiste en “*Educar y formar jóvenes solidarios, con sentido de pertenencia y respeto*”<sup>1</sup>.

El universo seleccionado son los grados 9, 10 y 11 de la institución educativa, Catumare la población a impactar es de 405 estudiantes y el tamaño de la muestra a trabajar son de 100 jóvenes cuyas edades oscilan entre los 14 y 20 años, distribuidos entre los géneros masculinos y femeninos.

A pesar de no ser necesario el manejo de información personal de los estudiantes como son nombres, direcciones o números telefónicos, la propuesta se registrará por la *Ley 1581 de 2012* sobre la protección de datos personales<sup>2</sup>.

El estudio permitirá conocer, el nivel de riesgo al cual están expuestos diariamente los estudiantes de la Institución Educativa, y a partir de los resultados obtenidos definir medidas de seguridad que les permita reducir las amenazas que estos dispositivos pueden generar.

La metodología implementada para el desarrollo del proyecto se basa en investigación de tipo cualitativa y cuantitativa, a través de encuestas, las cuales son herramientas utilizadas para obtener datos necesarios para el estudio.

---

<sup>1</sup> CATUMARE, Institución Educativa (10 de mayo de 2014). Visión & Misión. Obtenido de [http://colcatumare.edu.co/j3/index.php?option=com\\_content&view=category&id=28&Itemid=499](http://colcatumare.edu.co/j3/index.php?option=com_content&view=category&id=28&Itemid=499)

<sup>2</sup> MINTIC (6 de junio de 2018), Ley 1581 de 2012. Obtenido de [https://www.mintic.gov.co/portal/604/articles-4274\\_documento.pdf](https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf)

## INTRODUCCIÓN

El presente proyecto, guía al lector acerca del grado de vulnerabilidad a los que están expuestos continuamente los jóvenes de nuestra sociedad, al hacer uso de sus equipos celulares y los servicios de las redes sociales, los cuales permiten ampliar la capacidad de comunicación e interacción entre las personas y que por falta de un correcto asesoramiento, han desarrollado prácticas indebidas que representan una brecha de seguridad a su integridad como personas, exponiéndolas a peligros y/o ataques que pueden afectar su vida y entorno.

Para desarrollar el proyecto, se sigue los pasos definidos por la metodología de investigación de campo, que por sus características es perfectamente aplicable al tipo de estudio a realizar.

Inicialmente, se realiza una recopilación de información previa sobre la población a analizar, luego se realiza un análisis preliminar del procedimiento a diseñar para abordar la investigación, continúa con la aplicación de instrumentos diseñados para obtener inicialmente datos para el estudio, y se materializa los mecanismos contruidos para impactar a la muestra seleccionada, de tal forma que permita concientizar a la población de la muestra y así lograr un cambio en los hábitos inseguros, por último se aplica herramientas que permitan evaluar el impacto del mecanismo aplicado y se generan conclusiones al respecto.

## **1. PLANTEAMIENTO DEL PROBLEMA**

### **1.1. DESCRIPCIÓN DEL PROBLEMA**

Internet desde su aparición, ha evolucionado de ser un medio de consulta a través de una serie de equipos interconectados, a una plataforma de intercomunicación e interacción entre diferentes grupos sociales a nivel mundial, que ha abierto las puertas a un mundo infinito de posibilidades para todos.

A partir de esto, ha logrado masificar su utilización, a todos los niveles sociales y culturales de la población mundial, mediante el desarrollo e implantación de herramientas de fácil uso e interacción humana, que llega poblaciones de todas las edades y géneros.

Esta penetración de herramientas y su uso masivo, ha provocado una ola gigantesca de información que se transfiere, comparte, accede y divulga por la red y por los dispositivos a ella conectados.

A través de todos estos aspectos, los cuales están acompañados de avances tecnológicos, la humanidad ha modificado su estilo de vida y cultura de manera transversal dentro de ambientes sociales como son: el familiar, el laboral, el personal, el escolar y otros demás. Este cambio, se ha dado a través del uso de equipos de cómputo y de comunicación como son: portátiles, tablets, celulares, entre otros, apoyados por herramientas de comunicación como el correo, mensajería, chats, redes sociales y navegadores web.

Sin embargo, con la evidente penetración de toda esta tecnología a los círculos más privados y personales de la sociedad, se ha desarrollado a la par una subcultura de delitos y depravaciones de personas que consumen la información que fluye a través de la red en sus diferentes formas, como son texto, audio, imágenes y demás, y que están acompañadas a su vez de desinformación del usuario, malas prácticas y aumento de la confianza en el uso de herramientas y contenido generado.

Estos delitos y depravaciones, afectan a toda la población por igual sin distinción alguna; parte de los delitos desencadenan en delitos como: extorción, robo, abuso sexual, secuestros u homicidios, entre muchos más. Por lo tanto, se hace necesario tomar medidas que permitan disminuir las brechas de exposición al peligro al que se está expuesta la población a través de los distintos medios informáticos, herramientas y aplicaciones digitales disponibles en el mercado.

Algunas de las medidas que se pueden implementar para disminuir la exposición a peligros informáticos consisten en mecanismos de seguridad implantados directamente en los equipos y dispositivos, limitación en el uso de las tecnologías, concientización de los usuarios para el uso apropiado de equipos y herramientas entre muchas otras.

Por lo tanto, desde el desarrollo de este proyecto se apuesta por la concientización en la debida utilización de los medios y herramientas disponibles en el mercado con el objetivo de que los usuarios sean conscientes de las oportunidades, fortalezas y debilidades que conlleva el uso y distribución de contenido personal que producen en el desarrollo de su vida personal y social.

## **2. FORMULACIÓN DEL PROBLEMA**

¿Cómo, la socialización mediante charlas sobre seguridad informática, contribuye en el mejoramiento de las prácticas de seguridad y concientización de la población educativa de los grados 9, 10 y 11 de la Institución Educativa Catumare?

### 3. JUSTIFICACIÓN

En Colombia “el tercer país de América Latina en el uso de Smartphone (Semana, 2015)”, se está viendo una lenta pero constante penetración de la población al sector de tecnología y telecomunicaciones, es por eso que la expansión de la tecnología y su fácil accesibilidad por parte de la comunidad en general (MinTIC) ha provocado que un sector de la población, explote a una mayor velocidad esta oportunidad tecnológica.

Los grupos de jóvenes, cada vez a una edad más temprana, tienen ahora un mayor contacto con la Internet y las redes sociales, donde la capacidad de compartir información privada en espacios públicos ha debilitado las medidas de autoprotección, seguridad personal y familiar.

Esta tendencia se convierte en un foco de inseguridad en mayor parte para los jóvenes debido al aumento de los riesgos a su integridad, exponiendo delante de posibles atacantes información crítica que les permite determinar comportamientos, gustos, ubicaciones, parentescos familiares, hábitos, entre muchos otros aspectos de la vida personal, familiar y laboral, etc.

Por eso, es indispensable generar conciencia sobre este tipo de comunidades, debido a su capacidad de reconocimiento y comprensión sobre tecnología (MinTIC, Internet el mejor aliado de nuestros niños, 2017). Adicionalmente, ofrecer la posibilidad de expandir esta conciencia adquirida a otros miembros de sus grupos sociales y/o familiares, permitiría mitigar la materialización de riesgos relacionados con la seguridad informática y personal.

## **4. OBJETIVOS**

### **4.1. OBJETIVO GENERAL**

Evaluar el nivel de las medidas de seguridad informática que implementan los estudiantes de los grados 9, 10 y 11 de la Institución Educativa Catumare de la ciudad de Villavicencio, al momento de hacer uso de dispositivos Smartphone para compartir información en redes sociales u otros medios de transferencia de información personal.

### **4.2. OBJETIVOS ESPECÍFICOS**

- Realizar reconocimiento de la Institución Educativa, cómo está conformada, jornadas académicas, cantidad de estudiantes, y distribución de cursos.
- Elaborar plan de trabajo para socializarlo con el personal administrativo de la institución que incluya actividades, tareas, pruebas iniciales y finales, recursos necesarios, inconvenientes, responsables y tiempo de ejecución.
- Diseñar y ejecutar talleres de concientización, que permitan mejorar la cultura de la población en estudio, relacionados con el uso adecuado de las redes sociales y demás información personal a través de dispositivos móviles, permitiendo expandir este conocimiento al entorno social y familiar de los jóvenes.
- Fortalecer el conocimiento adquirido en el ámbito educativo y profesional, a través de charlas que permita generar un impacto positivo en las comunidades afectadas por el proyecto y que les permita tener la visión de nuevas estrategias a manejar por parte de los estudiantes de la Institución Educativa Catumare de la ciudad de Villavicencio.
- Generar y socializar entre las directivas de la Institución y la población estudiantil de los grados 9, 10 y 11, informe con los resultados obtenidos, y sus respectivas recomendaciones para mitigar los riesgos y vulnerabilidades de seguridad identificadas.

## **5. MARCO TEÓRICO**

### **5.1. MARCO REFERENCIAL**

El avance de la tecnología y la masificación de grandes volúmenes de información, la popularización del uso de equipos móviles como Smartphone, la fácil adquisición de paquetes de datos por parte de jóvenes estudiantes con el objetivo de acceder a este cumulo de información, ha incrementado de igual forma los riesgos de exponerse a esta tecnología. Es por esto, que la seguridad de la información es un tema que se debe conocer, manejar y mantener.

Los equipos móviles son usados para comunicarnos, enviar información de temas estudiantiles, familiares y sociales, cuyo contenido incluye fotografías, audios, videos, texto, direcciones de correos electrónicos, números de contacto entre muchos otros, para hacer uso de este contenido se requiere de aplicaciones y herramientas que se conectan a una serie de servicios en la web dentro de los cuales se almacenan nuestros datos personales permitiendo crear accesos “autorizados” a parte de nuestra información guardada en la memoria del teléfono o en la nube.

Mucha de nuestra información en estas aplicaciones y servicios está dispuesta para que criminales informáticos vigilen, tomen, roben y manipulen nuestros datos. Son muchos los casos de extorsiones que han sido resultado de hackeo de sus dispositivos móviles y ordenadores, e información compartida en las redes de datos.

Para desarrollar este proyecto se seguirá la metodología de investigación de campo cualitativa, a través de la cual se listan los siguientes pasos:

- Plantear el problema relacionado con el nivel de seguridad en el uso de equipos Smartphone
- Identificar espacios de trabajo
- Planificar fechas de actividades
- Diseñar estrategia de recolección de información
- Establecer población y tamaño de muestra
- Implementar pre-test sobre la muestra
- Procesar información recopilada
- Elaboración de charlas de socialización y sensibilización sobre seguridad informática
- Implementación de post-test
- Procesamiento de información recopilada en el post-test
- Divulgación de resultados, medidas y conclusiones
- Presentación de informes gerenciales a la administración de la Institución Educativa.



Como parte del proceso de comprensión del proyecto es necesario contar con criterios como:

**Smartphone en el proceso de aprendizaje y enseñanza:** la educación durante la última década ha sufrido un cambio en cuanto a las herramientas de apoyo utilizadas por los estudiantes permitiendo un mayor acceso al conocimiento generando un dinamismo en las estrategias pedagógicas y de enseñanza y aprendizaje de los diferentes grupos de estudiantes, independientemente de la edad o desarrollo cognitivo. De acuerdo con Silva Calpa y Alicia Cristina<sup>3</sup> *“Los procesos de aprendizaje están totalmente influenciados por el uso intensivo de las tecnologías (Rush, 2011), por lo cual es importante indagar cuál es la influencia del Smartphone”*

Las implementaciones de estos dispositivos generan discusión entre los diferentes grupos de opinión en donde se resaltan contradictores y quienes están a favor<sup>4</sup>. De un lado sirven como impulsores de la adquisición y exploración de conocimiento permitiendo generar nuevo pensamiento y para la contraparte resulta ser el mayor punto de distracción en las aulas de estudio<sup>5</sup>.

Las instituciones como los padres de familia son los directamente responsables de la orientación adecuada de los estudiantes en el uso adecuado y aprovechamiento de estas herramientas, para evitar que se conviertan en un punto de riesgo para la integridad y desarrollo de su persona, debido al alto nivel de popularidad e integración en la vida cotidiana resultando ser causa de actividades ilegales, explotación sexual, pornografía, acoso entre muchas otras<sup>6</sup>.

---

<sup>3</sup> SILVA CALPA, y otros (2017). Influencia del Smartphone en los procesos de aprendizaje y enseñanza. Obtenido de <https://www.sciencedirect.com/science/article/pii/S2215910X17300010>

<sup>4</sup> ORGANISTA SANDOVA, J. (2012). Apropiación y usos educativos del celular por estudiantes y docentes universitarios. Obtenido de <http://www.redalyc.org/pdf/155/15529662010.pdf>

<sup>5</sup> ESPECTADOR, El. (19 de 05 de 2015). No a los celulares en la escuela. Obtenido de <https://www.elespectador.com/noticias/educacion/no-los-celulares-escuela-articulo-561238>

<sup>6</sup> HENDERSON, C. (2016). El impacto de los teléfonos celulares en instituciones educativas. Obtenido de [https://techlandia.com/impacto-telefonos-celulares-instituciones-educativas- sobre\\_44439/](https://techlandia.com/impacto-telefonos-celulares-instituciones-educativas- sobre_44439/)

## 5.2. MARCO CONCEPTUAL

En el desarrollo del presente proyecto se hace necesario unificar conceptos que permitan obtener una mejor comprensión de los temas que se relacionan en el documento.

A continuación, se realiza una descripción contextualizadas de los conceptos:

**Ataque informático:** Es la materialización de un riesgo informático, que afecta la privacidad y/o disponibilidad de la información del estudiante, este puede generarse por la actuación de otro individuo o por software malicioso (Virus) que se instala en el celular o equipo de la víctima.

**Datos personales:** Consiste en información, que hace parte de la vida privada o familiar del estudiante, así como de miembros administrativos de la institución educativa (MinComercio, 2013).

**Delincuente informático:** Personas que realiza operaciones delictivas mediante el uso autorizado o forzado de dispositivos electrónicos como equipos de cómputo o equipos móviles, cuyo objetivo incluye robo, modificación, eliminación o extorsión, con fines personales o económicos (González, 2004), de la información, bienes u otro activo de los estudiantes víctimas.

**Delitos informáticos:** Son acciones realizadas a través de medios informáticos, que afectan la integridad de los estudiantes, docentes o administrativos de la Institución Educativa Catumare o cualquier tercero.

**Equipos/Dispositivo móviles:** Consiste en dispositivos electrónicos que son fácilmente transportables por la comunidad estudiantil, cuyo objetivo principal es el manejo de contenido multimedia (audio, fotos, videos y texto), llamadas telefónicas y/o videollamadas.

**Extorsión:** Se trata de la obligación contraída de manera forzada y sin autorización por algún miembro de la comunidad educativa de la Institución educativa, cuyo objetivo consiste en obtener un beneficio (económico, emocional, etc.) de modo ilícito (Colombia, 2018).

**Informática:** Conjunto de conocimiento técnico y científico perteneciente a la comunidad estudiantil, que permite el tratamiento de la información a través de dispositivos de cómputo (Carmen de Pablos, 2004).

**Institución educativa:** Conjunto de personas y bienes, cuya finalidad es prestar el servicio de formación educativa (MinEducación, 2004), a la comunidad perteneciente al Barrio Catumare y sus alrededores.

**Investigación cualitativa:** Método de recolección de información, aplicado dentro de la Institución Educativa Catumare, el cual está basado en criterios de calidad como

observación de comportamientos, tipos de respuestas dadas, y demás características personales asociadas a los integrantes de la comunidad educativa, y a partir de los cuales, se pueda obtener unos resultados específicos<sup>7</sup>. Hace uso de diversas herramientas como son: la observación, encuestas, entrevistas, entre otros

**Privacidad:** Condición que poseen los datos personales, perteneciente a cada miembro de la comunidad estudiantil de la Institución Educativa Catumare. Esta condición hace, que la información de las personas no sea divulgada a terceros de manera abierta.

**Riesgo:** se define como la probabilidad que se materialice una amenaza sobre los miembros de la Institución Educativa, hasta llegar a convirtiéndose en un desastre.

**Riesgo informático:** Probabilidad de que se presente un incidente informático sobre equipos de cómputo o dispositivos móviles pertenecientes a la comunidad estudiantil de la institución educativa.

**Smartphone / teléfonos inteligentes:** Consiste en dispositivos móviles, cuyo objetivo principal es la comunicación entre otros equipos. Adicionalmente, prestan servicios como conexión a Internet y uso de aplicaciones multimedia (audio, fotos, videos y texto).

**Tecnología:** Conjunto de conocimientos aplicados (Sánchez, 2012) a través de los cuales se han obtenidos herramientas, y mejoramiento de procedimientos que son utilizados e implementados en la cotidianidad por los miembros de la comunidad estudiantil.

**TIC, TICS:** (Tecnologías de la Información y de la comunicación) se refiere al área de las ciencias enfocadas en la información y las comunicaciones que facilitan la emisión, transmisión, acceso y manejo de la información digital<sup>8</sup>, producida y/o manejada por la comunidad estudiantil. Son características de las TICS:

- Inmaterialidad
- Interactividad
- Interconexión
- Instantaneidad
- Digitalización
- Transversalidad
- Innovación
- Diversidad
- Posibilidad de automatización

---

<sup>7</sup> MUNARRIZ, B. (1992). Técnicas y métodos en Investigación cualitativa. Obtenido de <https://ruc.udc.es/dspace/bitstream/handle/2183/8533/CC-02art8ocr.pdf>

<sup>8</sup> MINTIC. (2016). TIC. Obtenido de <http://tugimnasiacerebral.com/herramientas-de-estudio/que-son-las-tics-tic-o-tecnologias-de-la-informacion-y-la-comunicacion>

### 5.3. MARCO LEGAL

Debido a las condiciones especiales que poseen todos los miembros de la comunidad estudiantil de la Institución Educativa Catumare, y más aún, por su condición de estudiantes, los cuales en su mayoría son menores de edad, es necesario tener en cuenta los lineamientos y condiciones dadas por los organismos de protección para el manejo y protección de la información de ellos y de la Institución como tal.

El presente proyecto está enmarcado principalmente en el cumplimiento de las leyes para la protección de la información:

Artículo 15 de la Constitución Política de Colombia<sup>9</sup>, relacionado con la privacidad y el buen nombre.

Ley 599 de 2000. Del Código penal colombiano el cual contiene normas jurídicas punitivas del Estado Colombiano.

Ley 1273 de 2009. De la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1581 de 2012. Por medio de la cual se dictan disposiciones generales para la protección de datos personales.

Acuerdo No 03 de junio 16 de 2016, por el cual se aprueba y adopta la reestructuración del Manual de Convivencia de la Institución Educativa Catumare de la ciudad de Villavicencio.

---

<sup>9</sup> COLOMBIA, Constitución Política de (2003). Constitución Política de Colombia, Artículo 15. Obtenido de <http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15>

## 5.4. ESTADO DEL ARTE

A continuación, se describen algunos estudios, referentes al desarrollo pedagógico de los estudiantes a través de la utilización de dispositivos móviles en los ambientes escolares, los cuales permiten tener una perspectiva concreta sobre su uso y la problemática generada por las malas prácticas en el manejo de la información. A partir de esa información proporcionada, se puede orientar el estudio a desarrollar en el presente proyecto.

De acuerdo con Merino, E. & Caballero, J. *“los jóvenes utilizan la mayoría de las herramientas que presentan los teléfonos móviles. Sin embargo, las asociadas a la organización de los tiempos y tareas evidencian un nivel de uso incipiente. Los estudiantes utilizan los teléfonos móviles en distintos ámbitos de su vida personal, prevaleciendo sus interconexiones con sus pares a través del texto y en su mayoría lo consideran imprescindible. Los estudiantes declaran utilizarlo en su trabajo académico, sin embargo, lo reconocen como un potencial distractor ya que modifica el contexto de la clase, posicionándolos en redes sociales o en el ciberespacio, lo que los hace desatender su quehacer académico”*<sup>10</sup>.

De acuerdo con este estudio, los estudiantes han desarrollado habilidades comunicativas y de investigación a través de los medios tecnológicos dispuestos a su alcance, permitiéndoles acceder al contenido dispuesto en la web, así como compartir sus experiencias entre compañeros de clases y familiares. Sin embargo, el problema de esta tendencia, radica en que se realiza en medio de las actividades curriculares, lo que genera que el estudiante pierda la concentración requerida ante la oratoria del tutor o docente.

Según Córdoba Castrillón M. et al. *“Los estudiantes, en su mayoría, utilizan dispositivos tecnológicos para su uso personal, y les gustaría que todos los maestros transformaran sus estrategias didácticas hacia el uso de tecnologías en el aula de clase, utilizando múltiples dispositivos y aplicaciones que permitan clases más dinámicas y divertidas”*<sup>11</sup>.

Como se puede apreciar, resulta inherente el uso de medios tecnológicos dentro de los ambientes educativos, y su principal objetivo dentro de las aulas educativas es el de ser un apoyo en el desarrollo de los contenidos curriculares. Sin embargo, parte de la falla en este sistema, se debe a la poca apropiación de los tutores a hacer uso activo de estas tecnologías, permitiéndoles a los estudiantes crear espacios que son utilizados para establecer relaciones interpersonales a través de la interacción social.

---

<sup>10</sup> MERINO, E. C. (2017). El teléfono móvil y los estudiantes universitarios: Una. Pixel-Bit, 96

<sup>11</sup> CÓRDOBA CASTRILLÓN y Otros (2017). Estudiantes de la básica y media con respecto al uso de las TIC como herramientas. Trilogía Ciencia Tecnología Sociedad, 14.

Por su parte Carlos Figueroa<sup>12</sup> demuestra la manera de cómo los estudiantes de un determinado curso, hacen uso de dispositivos móviles en su mayoría *Smartphone* para la búsqueda de información, gracias a las características de los equipos móviles como son: portabilidad, conectividad a internet, usabilidad, convergencia de servicios, entre otros.

De acuerdo con el enunciado de Carlos Figueroa, es importante que toda la comunidad que conforma la Institución Educativa Catumare, se apropie de la utilidad que resulta esta tecnología y la implementen de manera activa, proactiva y responsable para el desarrollo de las actividades cotidianas dentro y fuera de las aulas.

Navaridas, Fermín; Santiago, Raúl & Tourón<sup>13</sup> exponen un estudio sobre la influencia de los dispositivos móviles en el proceso de aprendizaje de los estudiantes a través de diferentes ámbitos de la vida como son: afectivo/emocional, ético/social y cognitiva. Como resultado del estudio se concluye que estos dispositivos electrónicos potencializan el aprendizaje pedagógico mediante la mejora en la calidad.

El estudio aportado por los autores, reafirman la posibilidad de implementar de manera positiva los diferentes equipos móviles de comunicación que los estudiantes usan, para potencializar el desarrollo de las actividades curriculares de la Institución Educativa. Es de gran importancia que esta implementación, sea acompañada por profesores y padres de familia mediante una sana y apropiada orientación, que les permita a los estudiantes llevar a cabo buenas prácticas de uso, de tal manera que se disminuya la probabilidad de riesgo que puedan afectar su integridad.

---

<sup>12</sup> FIGUEROA PORTILLA, C. S. (2016). El uso del smartphone como herramienta para la búsqueda de información en los estudiantes de pregrado de educación de una universidad de Lima Metropolitana. Educación Vol. XXV, N° 49, 17.

<sup>13</sup> NAVARIDAS, F., Santiago, R., & Tourón, J. (2013). Valoraciones del profesorado del área de fresno (california central) sobre la influencia de la tecnología móvil en el aprendizaje de sus estudiantes. relieve, 19 (2), art. 4, 21.

## **6. DISEÑO METODOLÓGICO**

### **6.1. MÉTODO - ESTRUCTURA DE LA UNIDAD DE ANÁLISIS**

#### **6.1.1. Tipo de estudio.**

El presente proyecto, se enmarca a través de un desarrollo metodológico de campo, en donde el autor, se sitúa en el lugar de residencia de la población seleccionada, con el objetivo de recopilar información y datos directamente de la fuente, dentro del lugar de estudio.

Adicionalmente, se interactúa de manera no participante con la muestra seleccionada.

Los pasos a seguir, sugeridos por la metodología seleccionada son:

- Plantear el problema relacionado con el nivel de seguridad en el uso de equipos Smartphone
- Identificar espacios de trabajo
- Planificar fechas de actividades
- Diseñar estrategia de recolección de información
- Establecer población y tamaño de muestra
- Realizar encuesta sobre la muestra
- Tabular información recopilada
- Elaborar charla para socializar y sensibilizar a la población sobre seguridad informática en equipos móviles
- Aplicar nuevamente la encuesta
- Tabular información recopilada en la última encuesta
- Divulgar resultados, medidas y conclusiones
- Presentar informes a los directivos de la Institución Educativa.

#### **6.1.2. Tipo de investigación.**

Para abordar el tema planteado, se decide realizar una investigación mixta, tomando variables del tipo cuantitativa y cualitativa que permitan identificar perfiles, edades y sexos de la muestra seleccionada, así como los valores relacionados con cada una de estas variables.

### 6.1.3. Plan de trabajo.

Para cumplir con el objetivo del proyecto, se desarrollan las siguientes actividades:

- Inicialmente, se programa encuentro de trabajo con el rector de la Institución Educativa, cuyo objetivo es obtener los permisos correspondientes y viabilidad del proyecto a ejecutar en las instalaciones de la institución. Esto incluye socializar el proyecto, delimitar el alcance, los recursos necesarios, el personal de la institución a vincular y los grupos de estudiantes a los cuales aplica el proyecto.
- Socialización del proyecto con coordinadores de las diferentes sedes, donde se expone alcance, recursos, metodología de desarrollo basada en la aplicación de encuesta (al iniciar el proyecto y luego de realizada charla sobre seguridad), aplicación de charlas de concientización sobre seguridad informática a través de equipos móviles de estudiantes y tabulación de datos recopilados, en donde se presentará resultados obtenidos.
- Socialización con docentes de los grados noveno, décimo y undécimo de las diferentes sedes, donde se programa los espacios y horarios requeridos para cada actividad.
- El desarrollo de las actividades definidas, se divide en tres (3) secciones de trabajo con los diferentes grupos de estudiantes.

#### Primera

- Charla introductoria con estudiantes de cada curso, con duración de 15 minutos sobre actividad a realizar.
- Distribución, aplicación y posterior recolección de encuesta de percepción sobre prácticas personales de seguridad a través del uso de equipos móviles a cada estudiante del curso, con duración de 15 minutos.
- Tabulación de datos recopilados en encuestas aplicadas (1 semana).

#### Segunda

- Elaboración de charlas de concientización a la población incluida en el proyecto, sobre seguridad informática a través de los diferentes equipos de comunicación móvil del que hacen uso, cuyo objetivo es disminuir incidentes y peligros que se puedan presentar mediante este tipo de dispositivos, con duración de 45 minutos por grupo.
- Estas charlas se realizan en el auditorio de cada sede, contando con dispositivos de audio y proyección para tal fin.

#### Tercera

- Charla introductoria con estudiantes de cada curso, con duración de 15 minutos sobre actividad a realizar.
- Distribución de encuesta final, re-aplicación y recolección de formatos luego de aplicada



la encuesta de percepción, sobre prácticas personales de seguridad a través del uso de equipos móviles a cada estudiante, con duración de la actividad de 15 minutos.

- Tabulación de datos recopilados en encuestas aplicadas (2 semanas).
- Presentación de evidencias recopiladas (1 semana).
- Generación de informe con resultados obtenidos (2 días).
- Socialización de resultados con docentes, coordinadores y rectoría (2 horas).

## **6.2. DEFINICIÓN DE HIPÓTESIS**

La implementación de charlas de concientización sobre seguridad informática, permite a la población afectada, reducir la brecha de exposición, a riesgos y/o peligros informáticos que comprometan su seguridad personal, familiar y/o social.

## **6.3. VARIABLES**

### **6.3.1. Independientes.**

Hace referencia a las charlas sobre seguridad informática en equipos móviles como celulares, a través de las cuales se busca evaluar el nivel de seguridad que aplican los estudiantes de los grados 9, 10 y 11 de la Institución Educativa.

### **6.3.2. Dependientes.**

Mejorar el nivel de seguridad informática, sobre equipos móviles de la población en estudio de la Institución Educativa Catumare.

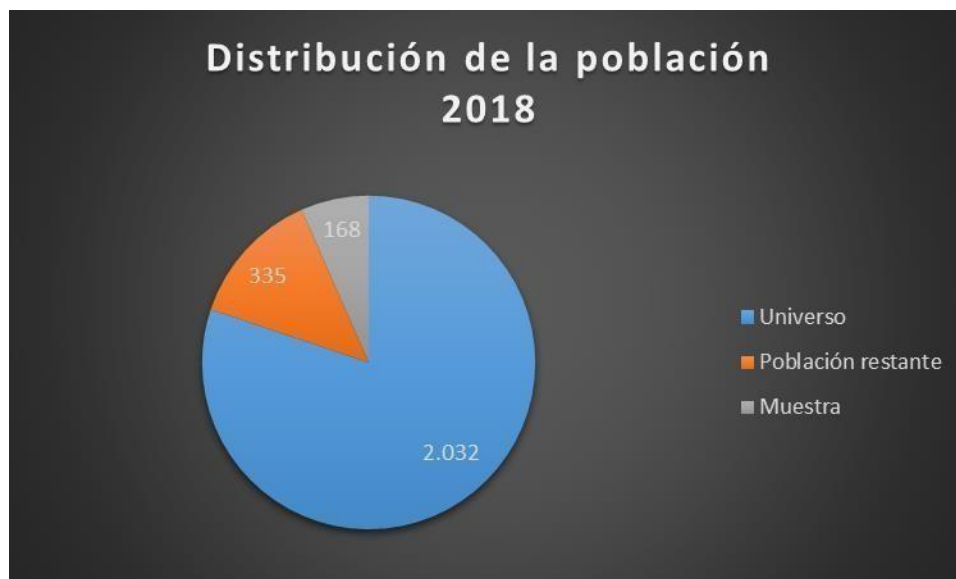
#### 6.4. UNIVERSO, POBLACIÓN Y MUESTRA

El universo seleccionado, es la totalidad de estudiantes matriculados en la Institución Educativa para el 2018, distribuidos en las 6 sedes que corresponde a 2.032 alumnos.

La población a evaluar, son los 503 estudiantes, inscritos en los grados 9, 10 y 11 de la Institución Educativa.

La muestra representativa, a trabajar es de 168 jóvenes (1/3 de la población), cuyas edades oscilan entre los 15 y 22 años, distribuidos entre los géneros masculinos y femeninos. Los candidatos seleccionados, aplicarán para las dos encuestas a realizar (Inicial y final).

*Figura 1. Distribución de la población objetivo*



Fuente. Inédita

#### 6.5. INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Por la naturaleza de la metodología, las herramientas propuestas para la recolección de datos son:

##### 6.5.1. Presentación.

Realizada por parte del autor del proyecto a los integrantes de la muestra seleccionada, con el objetivo de conocer de primera mano la población objetivo, adicionalmente se realizan encuentros con directivos y docentes de la institución para determinar la viabilidad de las actividades a desarrollar.

#### 6.5.2. Observación en campo.

A partir del cual, el autor obtiene datos relacionados con el desarrollo de la actividad.

#### 6.5.3. Encuestas.

Que permiten al autor, obtener información precisa. A partir de los resultados obtenidos, se obtiene una aproximación, a la solución del problema planteado de manera específica.

En principio, se diseña un modelo de encuesta con preguntas cerradas y una abierta (ver Tabla 1), que se aplica a la muestra para identificar cómo estos manejan ciertas prácticas de seguridad, la parte inicial de preguntas permiten caracterizar los integrantes de la muestra, un segundo grupo de preguntas permiten identificar la habilidad en el uso y el tipo de herramientas electrónicas, y un último grupo permite valorar el nivel de usabilidad que se tiene de las herramientas electrónicas.

Al finalizar, se aplica nuevamente el modelo de encuesta previamente usado, que permitirá evaluar el nivel de aceptación de las charlas impartidas, la concientización de las medidas de seguridad socializadas y el grado de seguridad que han adoptado los participantes de la muestra, luego de las charlas sobre seguridad.

**Tabla 1. Formato encuesta**

CARACTERIZACIÓN ENCUESTADO											
Grado/Curso		Edad		Sexo		Estrato Social					
IDENTIFICACION EQUIPO MOVIL											
ID	PREGUNTAS										
1.	¿Cuenta con teléfono móvil?		Si				No				
2.	¿Qué tipo de teléfono móvil tiene?		Básico		Smartphone			Tablet con Simcard			
3.	¿Instala las actualizaciones disponibles del equipo celular (App y sistema operativo)?		Si				No				
CONECTIVIDAD											
4.	¿Tiene conexión a Internet constante?		Wifi		Plan de datos			No			
5.	¿Cuenta con plan de datos?		Prepago		Postpago			No			
6.	¿Cuenta con plan de voz?		Prepago		Postpago			No			
USO											
7.	¿Utiliza el equipo dentro del salón mientras está en clases?		Si				No				
8.	¿Con qué frecuencia hace uso del equipo móvil?		Siempre	Muchas veces	Con frecuencia	A veces)	Alguna vez	Nunca			
9.	¿Qué uso le da al equipo móvil?		Califique del 0 al 10, siendo "0" nada y "10" mucho								
	Uso de chat		Consulta de tareas o actividades			Cámara de video		Juegos			
	Cámara fotográfica		Reproductor de música			Radio					
10.	¿Qué tipo de contenido consume en internet?		Humor	Sexual	Académico	Afectivo	Cultura gral				
11.	¿Qué red social consulta con más frecuencia con su equipo celular?		Facebook	Twitter	Google +	Linkedin	Otra:				
12.	¿Instala software por fuera de la Play store, y App Store?		Si	¿Cuál sitio?					No		
13.	¿Tiene implementado mecanismo de seguridad para acceder a su equipo?		Patrón	Huella	Facial	Números	No tiene				
14.	¿Qué grado de dificultad tiene el mecanismo de seguridad configurado en su celular?		Alto	Medio	Bajo	No tiene					
15.	¿Comparte fotografías con personas que no conoce personalmente?		Si				No				
16.	¿Comparte imágenes privadas a otra persona?		Si				No				
17.	¿A compartido imágenes privadas de tipo sexual a otra persona?		Si				No				
18.	¿Qué tan importante le resulta saber, lo que hagan otros con la información compartida de su parte?		Mucho	Algo	Poco	Nada	No lo había pensado	No			
19.	¿Su equipo celular ha sido infectado por virus?		Si				No				
20.	¿Tiene instalado software antivirus en su equipo móvil?		Si				No				
21.	¿Hace copia de la lista de contactos de su equipo móvil?		Si	Cómo:					No		
22.	¿Hace copia de las fotos de su equipo móvil?		Si	Cómo:					No		
23.	¿Cuántas personas conocen la clave o patrón de acceso a su celular?		0	1	2	3	4	5	Más		
24.	¿Controla el contenido que publica en redes sociales como Facebook u otros?		Si				No				
25.	¿Utiliza para conectarse a Internet redes públicas abiertas?		Si				No				
26.	¿Le han pedido algún tipo de retribución o pago a cambio de no publicar o difundir información personal ?		Dinero	Artículos	Abuso personal	Abuso sexual	No				
27.	¿Tiene alguna observación?										

Fuente. Inédita

## **6.6. FASES DE LA METODOLOGÍA**

A continuación, se describe las fases de la metodología a desarrollar, con las cuales se busca obtener los resultados de la investigación de campo.

### **6.6.1. Preliminar.**

Realizar levantamiento de información sobre la Institución Educativa, relacionada con jornadas académicas, cantidad de estudiantes, y distribución de cursos.

Para desarrollar esta fase, se realiza reuniones con el personal administrativo y docentes, buscando recopilar datos de la población estudiantil matriculada durante el presente año académico, con ello determinar la muestra a utilizar. Adicionalmente, se debe obtener información relacionada con la conformación de la Institución Educativa Catumare.

### **6.6.2. Introductoria.**

Elaborar plan de trabajo para socializarlo con el personal administrativo de la Institución Educativa que incluya actividades, tareas, pruebas iniciales y finales, recursos necesarios, inconvenientes, responsables y tiempo de ejecución.

Para el desarrollo de esta fase, se realiza mesa de trabajo donde se expone las actividades programadas a partir de la fase anterior, con el objetivo de encontrar la aceptación del plan de trabajo.

### **6.6.3. Desarrollo.**

Diseñar y ejecutar mecanismos de concientización, que permitan mejorar la cultura de la población en estudio, relacionada con el uso de dispositivos móviles, redes sociales y demás información personal de los estudiantes de la Institución Educativa, permitiendo expandir este conocimiento al entorno social y familiar de los jóvenes.

Para el desarrollo de esta etapa, se diseñan folletos donde se manejen temas relacionados con seguridad y privacidad.

Fortalecer el conocimiento adquirido en el ámbito educativo y profesional, a través de charlas que permita generar un impacto positivo en las comunidades afectadas por el proyecto y que les permita tener la visión de nuevas estrategias a manejar por parte de los estudiantes de la Institución Educativa Catumare de la ciudad de Villavicencio.

Estas charlas, se realizan con el objetivo de fortalecer la información distribuida mediante los folletos informativos. El contenido a tratar cuenta con la aprobación de las directivas de la institución, y hacen uso de herramientas tecnológicas como equipos de cómputo y videobeams, que permiten llegar a un mayor número de estudiantes por grupos.

#### 6.6.4. Finales.

Generar y socializar entre las directivas de la institución y la población estudiantil de los grados 9, 10 y 11, un informe con los resultados obtenidos, y sus respectivas recomendaciones para mitigar los riesgos y vulnerabilidades de seguridad identificadas.

Para los estudiantes participantes en la muestra, se entrega volantes informativos, en donde se informe los resultados del estudio de manera general. Mientras que, para el personal directivo, se presentan informes estadísticos con los resultados obtenidos y un análisis de los datos. Así mismo, se genera un informe que incluye las conclusiones del proyecto luego del análisis de la información.

## 7. LA INSTITUCIÓN

Ubicado en el barrio Catumare en la ciudad de Villavicencio Meta, inició como Escuela Catumare en el año de 1993 en la caseta comunal del barrio. En 1995 se trasladaron para instalaciones propias construidas por la alcaldía de la ciudad y para 1997 la escuela pasó a ser colegio durante el gobierno del señor Alfonso Ortiz Bautista.

En el año 2001 le fue entregado por parte de la alcaldía de Villavicencio el terreno donde se construyó la sede campestre del colegio para el año 2003.

En el año 2001 se inició el proceso de fusión de las sedes Nuevo Horizonte, San Jorge y Rochela, bajo la razón social de Colegio Departamental Catumare.

En el año 2012 cambia nuevamente su razón social a Institución Educativa Catumare.

Actualmente, el Colegio Departamental Catumare, bajo la dirección del señor rector Pedro Luis García García, está conformado por seis (6) sedes (*Principal, Campestre, San Jorge, Nuevo Horizonte, León XIII y Rochela*), y cuenta con convenios con el SENA para diferentes especialidades técnicas. Adicionalmente, capacita a población en extra edad y adultos en su jornada nocturna. La institución, cuenta con tres (3) jornadas académicas “Mañana”, “tarde” y “noche”, que albergan cerca de 2000 estudiantes anualmente.

La población de estudiantes de la institución, está distribuida de la siguiente manera:

Tabla 2. Distribución de cursos

Grado	Curso	Estudiantes	Grado	Curso	Estudiantes
Primero	1	35	Sexto	1	39
	2	34		2	38
	3	35		3	38
	4	35		4	39
	5	34		5	40
Segundo	1	36	Séptimo	6	41
	2	37		1	40
	3	35		2	40
	4	35		3	41
	5	35		4	39
Tercero	1	35	Octavo	5	35
	2	35		6	36
	3	34		1	42
	4	35		2	43
	5	36		3	35
Cuarto	1	36	Noveno	4	36
	2	36		5	34
	3	34		1	43
	4	35		2	43
	5	35		3	42
Quinto	1	32	Décimo	4	41
	2	35		5	40
	3	35		1	45
	4	35		2	44
	5	34		3	48
			Undécimo	4	36
				1	46
				2	43
				3	32

Fuente: Institución educativa



## 8. CRONOGRAMA DE ACTIVIDADES

A continuación, se relaciona la distribución de actividades de acuerdo con las fases sugeridas por la metodología para la ejecución del proyecto.

**Tabla 3. Cronograma de actividades**

FASE	ACTIVIDAD	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6
PREMILITAR	Revisión documental	x					
	Investigación sobre el uso de los métodos de protección de sistemas y dispositivos móviles	x					
	Investigación sobre el uso de herramientas para técnicas de encriptado de información	x					
	Investigación sobre el uso de diferentes tipos de amenazas a los sistemas, como son los virus, los troyanos, el spyware y los rootkits	x					
INTRODUCTORIA	Generar la logística necesaria para la intervención ante los grupos seleccionados de estudiantes de la Institución Educativa Catumare de la ciudad de Villavicencio.		x				
	Acordar fechas y horarios con las directivas de la Institución Educativa Catumare de la ciudad de Villavicencio, para las entrevistas y el desarrollo de las encuestas descriptivas		x				
	Preparar el material didáctico presentaciones móviles, folletos, volantes etc.		x				
	Acordar fechas y horarios con las directivas de la Institución Educativa Catumare de la ciudad de Villavicencio para realizar las capacitaciones requeridas.		x				
	Determinar fechas y horarios para evaluar el conocimiento adquirido por los grupos seleccionados de estudiantes de la Institución Educativa Catumare de la ciudad de Villavicencio.		x				
DESARROLLO	Ejecutar entrevistas y encuesta descriptiva inicial			x			
	Ejecutar las capacitaciones.				x	x	
	Ejecutar 2da encuesta descriptiva Final.					x	
	Desarrollar tablas de valorización de aprendizaje.					x	
FINAL	Generar y socializar un informe en el que se describa el resultado obtenido, y sus respectivas recomendaciones para mitigar los riesgos y vulnerabilidades.						x

Fuente. Inédita

## 9. DESARROLLO DE LA METODOLOGÍA

A continuación, se relacionan los resultados obtenidos al aplicar cada fase de la metodología de campo seleccionada y descrita en la sección 6.6.

### 9.1. PRELIMINAR

Los resultados obtenidos de esta fase, se presentan en la sección 7, en donde se relaciona la distribución poblacional de la institución en sus diferentes sedes, luego de llevarse a cabo reuniones con personal administrativo de la sede principal.

### 9.2. INTRODUCTORIA

Dentro de las actividades realizadas para esta fase, se define el cronograma de actividades (Ver sección 8), en donde se contó con el apoyo y aprobación de los coordinadores de disciplina (mañana / tarde), quienes evaluaron y dieron viabilidad a la distribución de las actividades relacionadas en la Tabla 4. Adicionalmente, se acordó con el departamento de ayudas educativas, el préstamo de un videobeam en las fechas relacionadas en el cronograma.

**Tabla 4. Programación de actividades fase de desarrollo**

FASE	ACTIVIDAD	SEPT	OCT	NOV
DESARROLLO	Ejecutar entrevistas y encuesta descriptiva inicial			
	9-1, 9-2	Sept 06		
	9-3, 9-4	Sept 07		
	9-5, 10-1	Sept 13		
	10-2, 10-3	Sept 14		
	10-4, 11-1	Sept 21		
	11-2, 11-3	Sept 22		
	Ejecutar las capacitaciones.			
	9-1, 9-2		Oct 12	
	9-3, 9-4		Oct 19	
	9-5, 10-1		Oct 26	
	10-2, 10-3			Nov 02
	10-4, 11-1			Nov 09
	11-2, 11-3			Nov 16
	Ejecutar 2da encuesta descriptiva Final.			
	9-1, 9-2			Nov 19
	9-3, 9-4			Nov 20
	9-5, 10-1			Nov 21
	10-2, 10-3			Nov 22
	10-4, 11-1			Nov 23
	11-2, 11-3			Nov 27
	Desarrollar tablas de valorización de aprendizaje.			Nov 28
				Nov 30

Fuente. Inédita

### **9.3. DESARROLLO**

Para esta fase de desarrolló un folleto tamaño carta a 3 columnas (ver ANEXO A - FOLLETO), en donde se brinda información relacionada con temas de seguridad y medidas de prevención, el cual fue distribuido y socializado con los estudiantes de los 3 grados (noveno, decimo y undécimo) de la Institución Educativa Catumare. Adicionalmente, se hizo uso de memofichas (ver ANEXO B - MEMOFICHAS) que se entregaron a los estudiantes para que hicieran comentarios desde su perspectiva, sobre la ficha entregada.

También se elaboró presentación en Power Point, que se socializó a los estudiantes dentro de las charlas realizadas (ANEXO C – PRESENTACIÓN).

De acuerdo con la percepción obtenida por parte de los diferentes grupos de estudiantes (ver ANEXO D - FORMATO DE ASISTENCIA), en general muestran interés por el tema y se apersonan de las distintas temáticas expuestas en la presentación. Haciendo algunos estudiantes intervenciones sobre sus experiencias personales al respecto (ver ANEXO E - GALERIA FOTOGRÁFICA).

El resultado de la implementación de estos mecanismos de transmisión de información, se refleja en las respuestas dadas en la primera evaluación de percepción (ver ANEXO F - ENCUESTA INICIAL APLICADA) comparándola con la misma aplicada por segunda vez (ver ANEXO G - ENCUESTA FINAL). Al finalizar la aplicación de esta encuesta se realizó tabulación de los datos, y los resultados de esta, se relacionan en la sección 10.

### **9.4. FINALES**

Como producto final del proyecto aplicado, se han desarrollado y socializado para la población estudiantil perteneciente a la muestra, un folleto con conclusiones (ver ANEXO H – FOLLETO DE RESULTADOS), en donde se relaciona los resultados pertenecientes a la tabulación de las respuestas entre la encuesta inicial y la final.

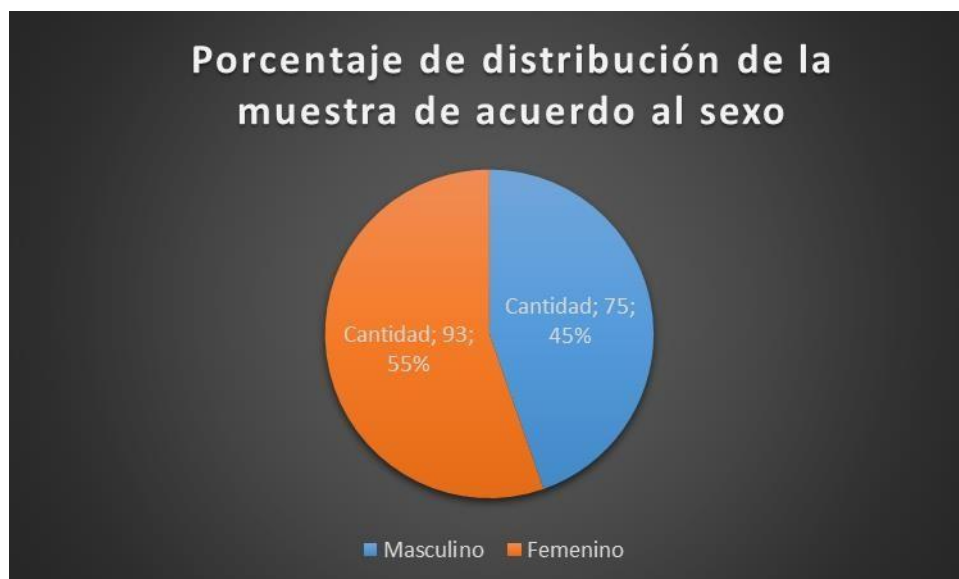
También se elabora y presenta informe ejecutivo a los directivos y profesores de la institución donde se les informa los resultados obtenidos del proyecto (ANEXO I – INFORME EJECUTIVO)

## 10. RESULTADOS OBTENIDOS DE LA ENCUESTA

A continuación, se relacionan los resultados obtenidos luego de aplicada la encuesta de manera inicial y posteriormente, después de realizadas las charlas sobre seguridad informática.

Con relación a la caracterización de la población encuestada, el porcentaje de distribución de acuerdo al género, se da de acuerdo con la Figura 2.

*Figura 2. Porcentaje de distribución de la muestra de acuerdo al sexo*

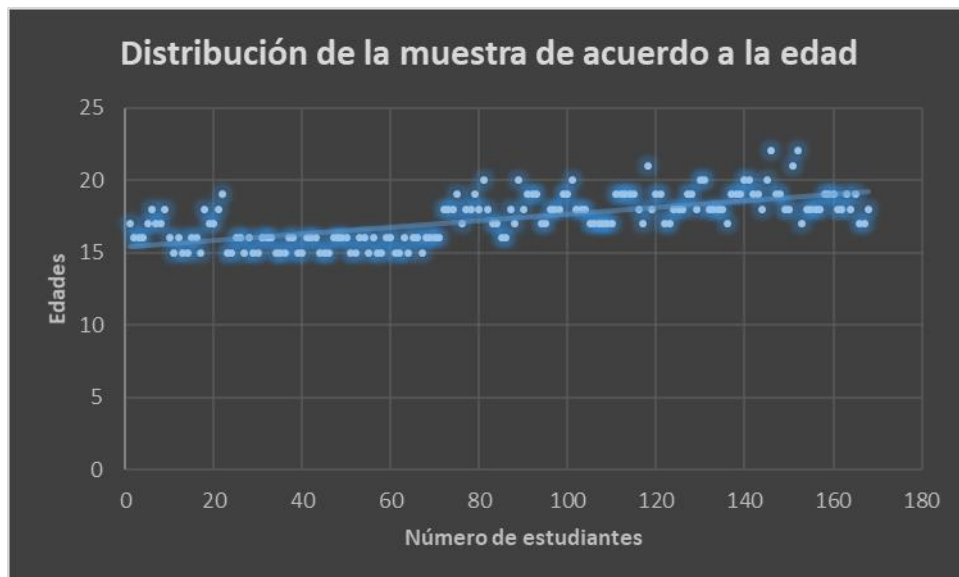


Fuente. Inédita

La Figura 2 muestra que la muestra seleccionada está conformada mayormente por estudiantes femeninas (55%), esto podría indicar que este tipo de población es más vulnerable a incidentes de seguridad informática debido a que están más en contacto con las redes sociales y divulgación de contenido visual como fotografías.

De acuerdo con la edad informada por los participantes de la muestra, se evidencia en la Figura 3.

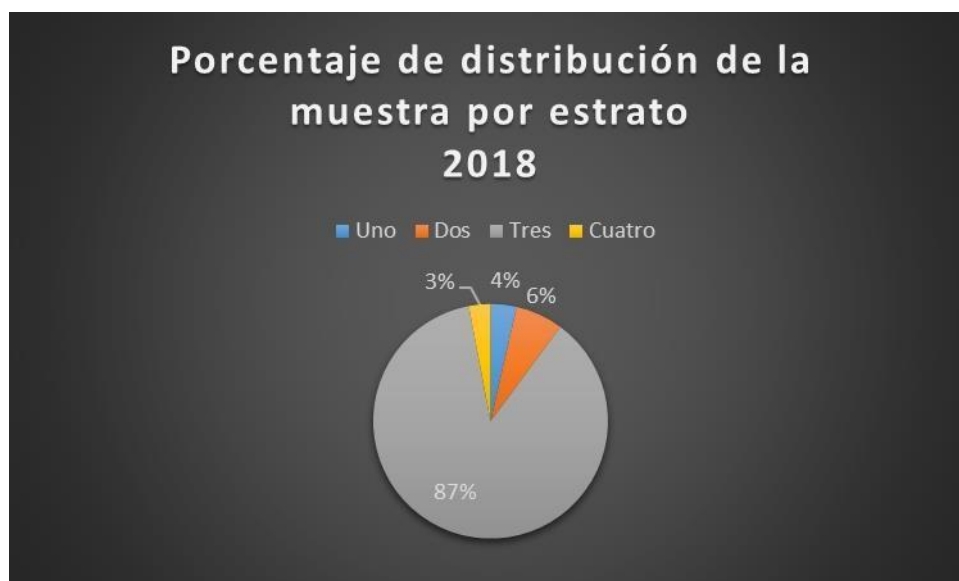
Figura 3. Distribución de la muestra de acuerdo a la edad



Fuente. Inédita

De acuerdo con el porcentaje de distribución de la población encuestada por estrato socio-económico, la mayoría de estudiantes son de estrato social 3.

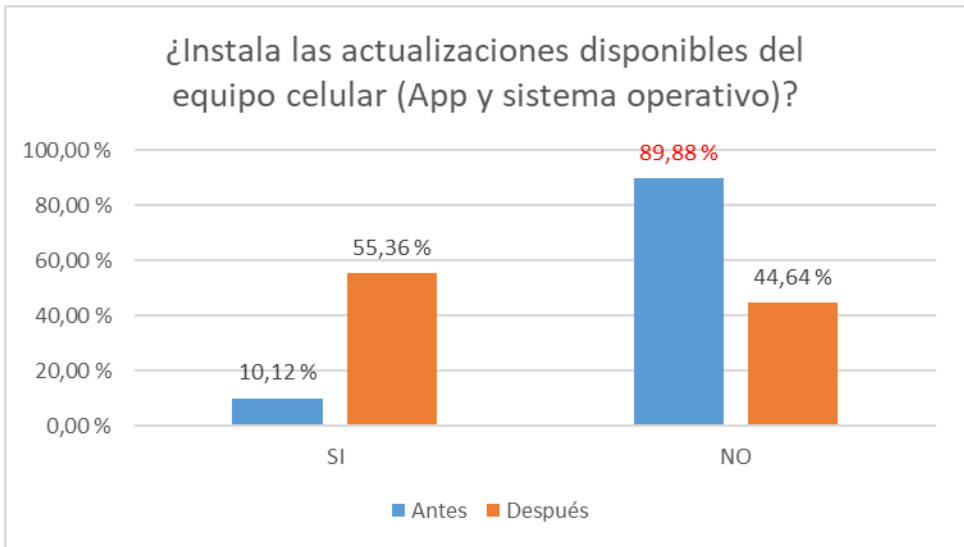
Figura 4. Distribución de la muestra por estrato socio-económico



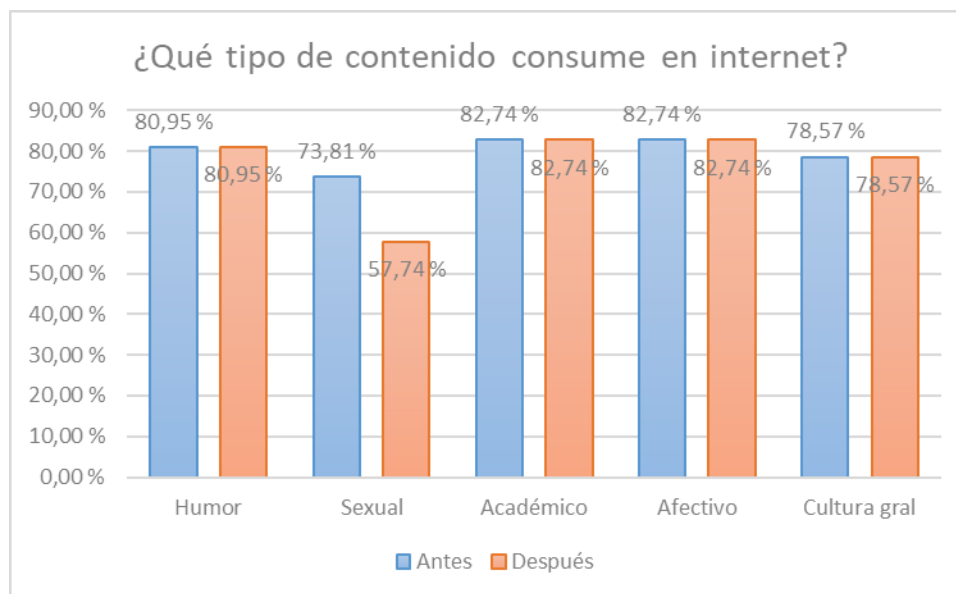
Fuente. Inédita

## 10.1. TABULACIÓN PRIMERA ENCUESTA

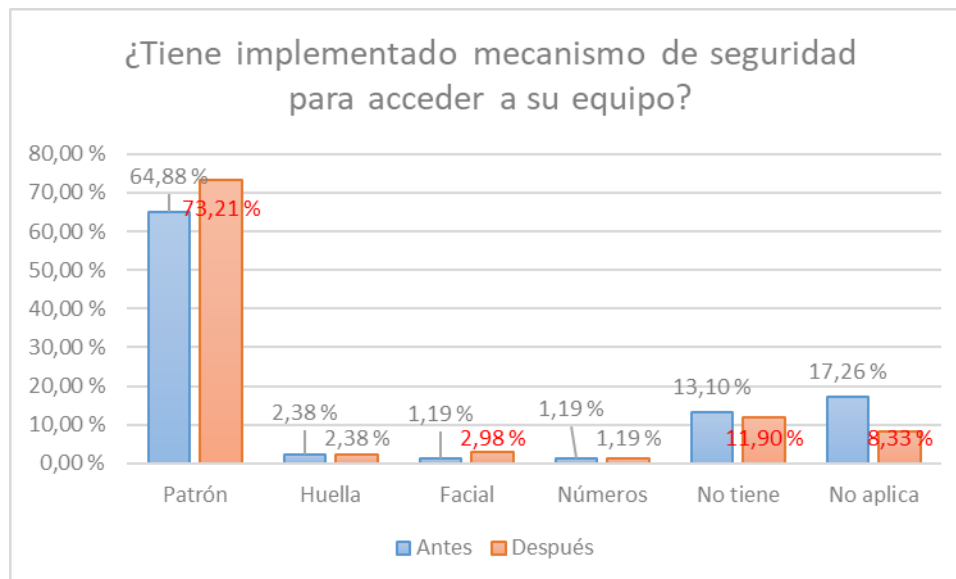
Tabla 5. Tabulación primera encuesta aplicada

ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS									
1.	¿Cuenta con teléfono móvil?	Si (87,50) No (12,50)	El 87,50% de los estudiantes tienen celulares									
2.	¿Qué tipo de teléfono móvil tiene?	Básico (4,76) Smartphone (79,17) Tablet con Simcard (3,57) No (12,50)	El 79,17% de los estudiantes cuentan con equipos Smartphone con capacidad de conexión a internet									
3.	¿Instala las actualizaciones disponibles del equipo celular (App y sistema operativo)?	Si (10,12) No (89,88)	El 89,88% de estudiantes no realiza las actualizaciones del sistema, cuando el fabricante libera mejoras para el sistema operativo.									
<div><p>¿Instala las actualizaciones disponibles del equipo celular (App y sistema operativo)?</p><table><thead><tr><th>Respuesta</th><th>Antes (%)</th><th>Después (%)</th></tr></thead><tbody><tr><td>SI</td><td>10,12 %</td><td>55,36 %</td></tr><tr><td>NO</td><td>89,88 %</td><td>44,64 %</td></tr></tbody></table></div>				Respuesta	Antes (%)	Después (%)	SI	10,12 %	55,36 %	NO	89,88 %	44,64 %
Respuesta	Antes (%)	Después (%)										
SI	10,12 %	55,36 %										
NO	89,88 %	44,64 %										
4.	¿Tiene conexión a Internet constante?	Wifi (22,62) Plan (63,10) No (14,29)	El 63,10% de los estudiantes cuentan con un plan de datos (prepago o postpago) que les permite estar conectados a Internet y demás servicios									
5.	¿Cuenta con plan de datos?	Prepago (31,55) Postpago (49,40) No (19,05)	El 49,40% de los estudiantes cuenta con planes postpago que les permite tener acceso constante a Internet									
6.	¿Cuenta con plan de voz?	Prepago (32,74) Postpago (50,00) No (17,26)	El 50,00% de los estudiantes cuenta con plan de voz									
7.	¿Utiliza el equipo dentro del salón mientras está en clases?	Si (51,19) No (48,81)	El 51,19% de los estudiantes hace uso del equipo celular dentro de las aulas de clase mientras reciben la cátedra									

ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
8.	¿Con qué frecuencia hace uso del equipo móvil?	Siempre (0,00) Muchas veces (73,21) Con frecuencia (7,74) A veces (1,79) Alguna vez (0,00) Nunca (17,26)	El 73,21% de estudiantes están constantemente conectados y al tanto de lo que sucede a través de los equipos móviles
9.	¿Qué uso le da al equipo móvil?	Redes sociales (82,74) Fotografía (87,50) Consultas (82,74) Reproductor (82,74) Video (82,74) Radio (5,36) Juegos (82,74)	El 87,50% de los estudiantes hace uso del equipo móvil para toma de fotografías principalmente.
10.	¿Qué tipo de contenido consume en internet?	Humor (80,95) Sexual (73,81) Académico (82,74) Afectivo (82,74) Cultura Gral (78,57)	El 82,74% de estudiantes hacen uso del equipo móvil para desarrollar trabajos académicos y contenido afectivo.

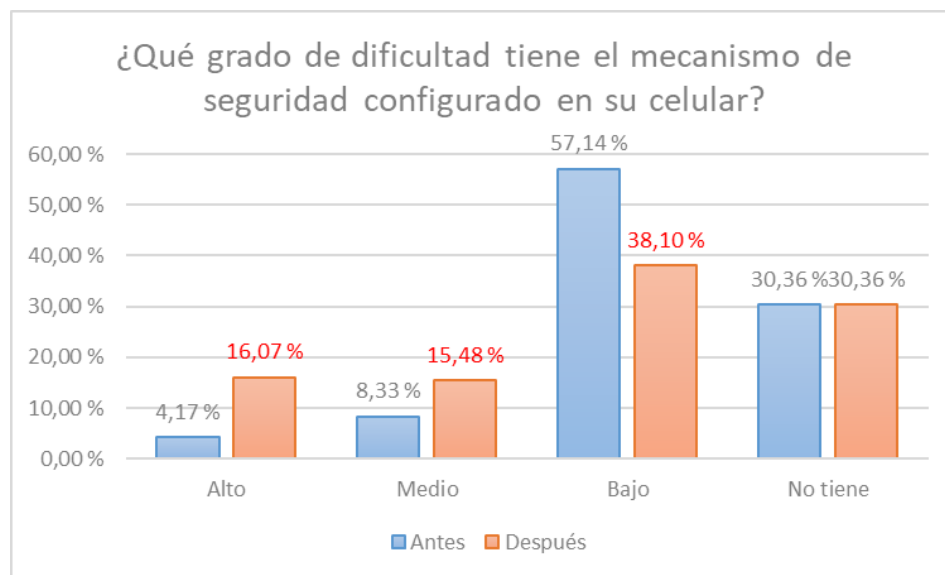


ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
11.	¿Qué red social consulta con más frecuencia con su equipo celular?	Facebook (63,69) Twitter (16,67) Google + (2,38) No (17,26)	El 63,69% de los estudiantes hacen uso de la red social Facebook para interactuar con otras personas.
12.	¿Instala software por fuera de la Play store, y App Store?	Si (35,12) No (64,88)	El 64,88% de los estudiantes están expuestos a software no autorizado por la empresa fabricante del sistema.
13.	¿Tiene implementado mecanismo de seguridad para acceder a su equipo?	Patrón (73,21) Huella (2,38) Facial (2,98) Números (1,19) No tiene (11,90) No aplica (8,33)	El 11,90% de estudiantes habilitaron algún mecanismo de seguridad para protección al acceso al equipo

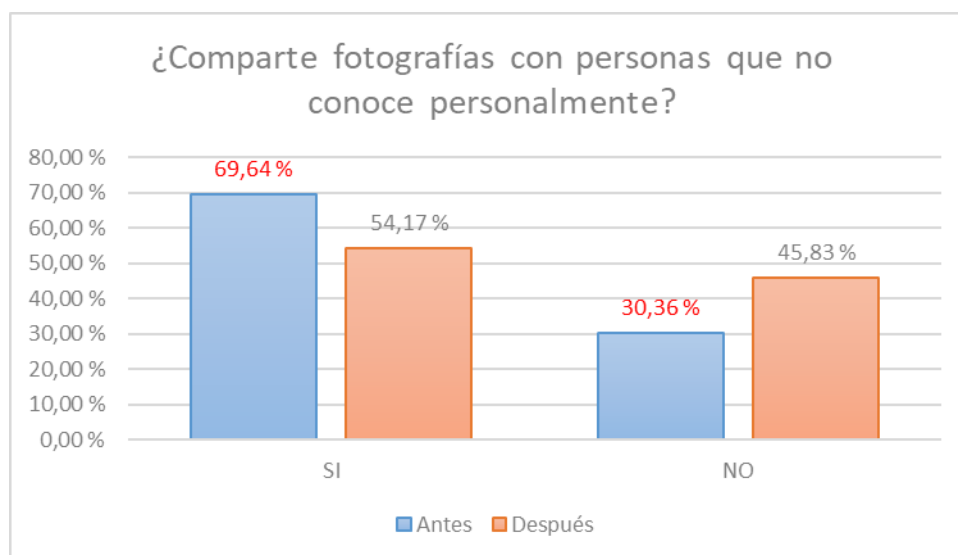




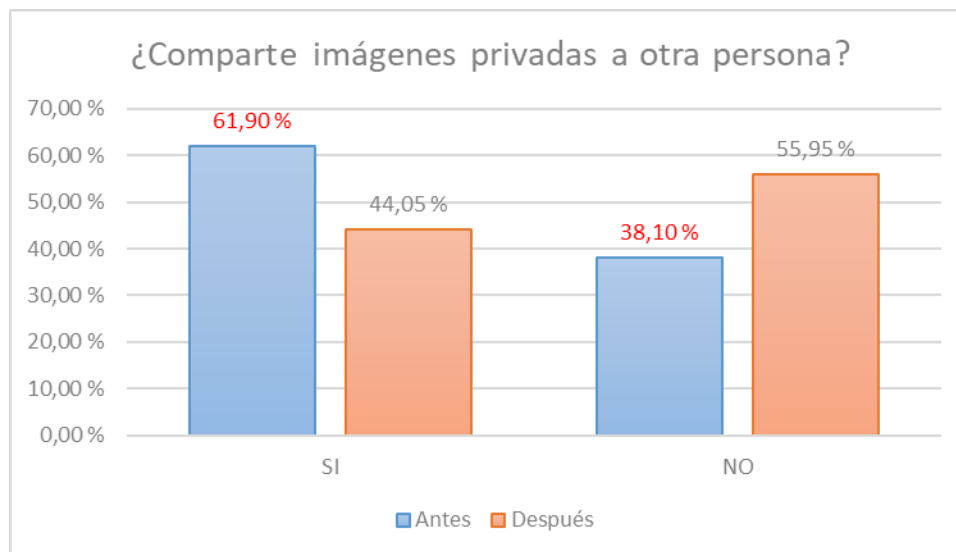
ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
14.	¿Qué grado de dificultad tiene el mecanismo de seguridad configurado en su celular?	Alto (16,07) Medio (15,48) Bajo (38,10) No tiene (30,36)	El 38,10% de estudiantes mejoró su patrón de seguridad.



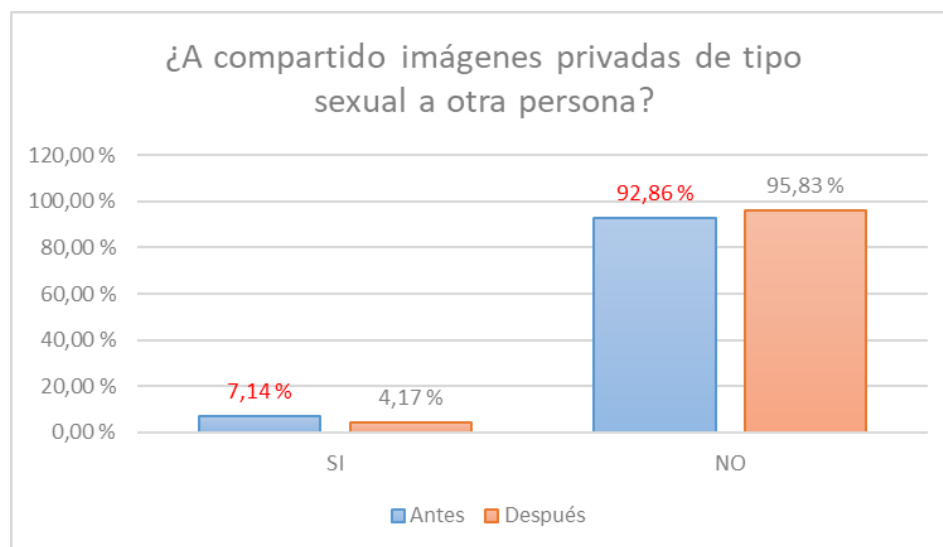
15.	¿Comparte fotografías con personas que no conoce personalmente?	Si (69,64) No (30,36)	El 69,64% de estudiantes están expuestos a ser víctimas de delitos por parte de personas desconocidas.
-----	---	--------------------------	--



ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
16.	¿Comparte imágenes privadas a otra persona?	Si (61,90) No (38,10)	El 61,90% de los estudiantes están expuestos a delitos como extorsión, abuso, pornografía al compartir imágenes de contenido privado

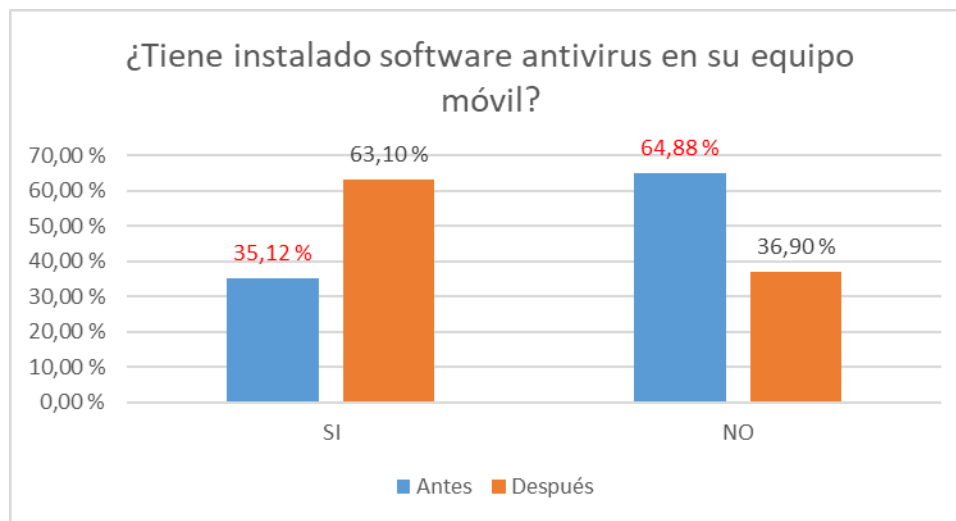


17.	¿Ha compartido imágenes privadas de tipo sexual a otra persona?	Si (7,14) No (92,86)	El 7,14% de los estudiantes están expuestos a delitos como explotación sexual, abuso, pornografía, al exponer imágenes de contenido privado
-----	---	-------------------------	---

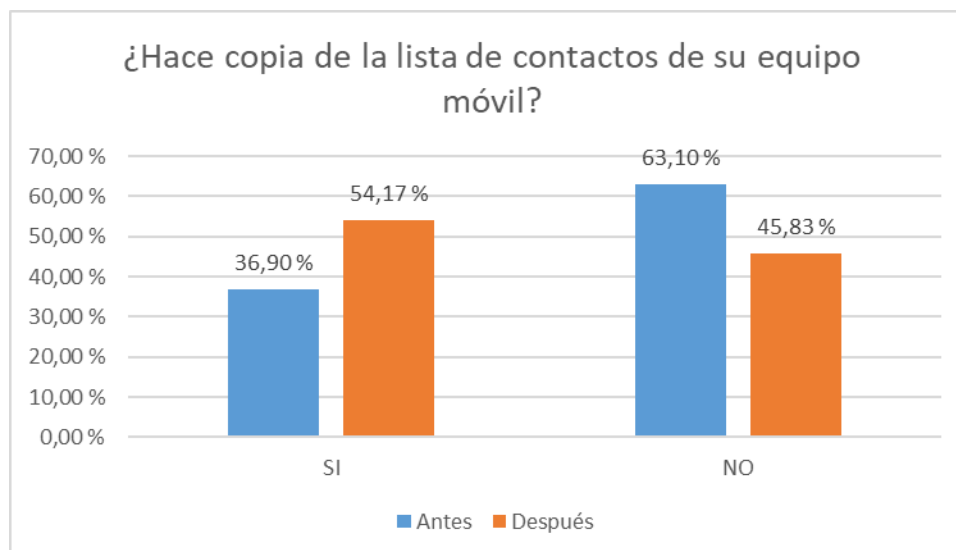


ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS																					
18.	¿Qué tan importante le resulta saber, lo que hagan otros con la información compartida de su parte?	Mucho (1,79) Algo (0,00) Poco (70,24) Nada (0,00) No lo había pensado (10,71) No (17,26)	Un 70,24% de los estudiantes están expuestos a delitos contra su persona debido a la poca importancia que le da al contenido que comparte, sin estar al tanto de las posibles consecuencias que se puedan presentar																					
<div><p>¿Qué tan importante le resulta saber, lo que hagan otros con la información compartida de su parte?</p><p>The bar chart displays the percentage of students for each response category, comparing 'Antes' (Before) in blue and 'Después' (After) in orange. The y-axis represents the percentage from 0,00% to 80,00%.</p><table><thead><tr><th>Respuesta</th><th>Antes (%)</th><th>Después (%)</th></tr></thead><tbody><tr><td>Mucho</td><td>1,79%</td><td>1,79%</td></tr><tr><td>Algo</td><td>0,00%</td><td>47,02%</td></tr><tr><td>Poco</td><td>70,24%</td><td>32,14%</td></tr><tr><td>Nada</td><td>0,00%</td><td>0,00%</td></tr><tr><td>No lo había pensado</td><td>10,71%</td><td>1,79%</td></tr><tr><td>No</td><td>17,26%</td><td>17,26%</td></tr></tbody></table></div>				Respuesta	Antes (%)	Después (%)	Mucho	1,79%	1,79%	Algo	0,00%	47,02%	Poco	70,24%	32,14%	Nada	0,00%	0,00%	No lo había pensado	10,71%	1,79%	No	17,26%	17,26%
Respuesta	Antes (%)	Después (%)																						
Mucho	1,79%	1,79%																						
Algo	0,00%	47,02%																						
Poco	70,24%	32,14%																						
Nada	0,00%	0,00%																						
No lo había pensado	10,71%	1,79%																						
No	17,26%	17,26%																						
19.	¿Su equipo celular ha sido infectado por virus?	Si (35,12) No (64,88)	El 35,12% de los estudiantes han sido afectados por infección de su equipo móvil que puede generar pérdida o robo de la información alojada en el equipo móvil																					

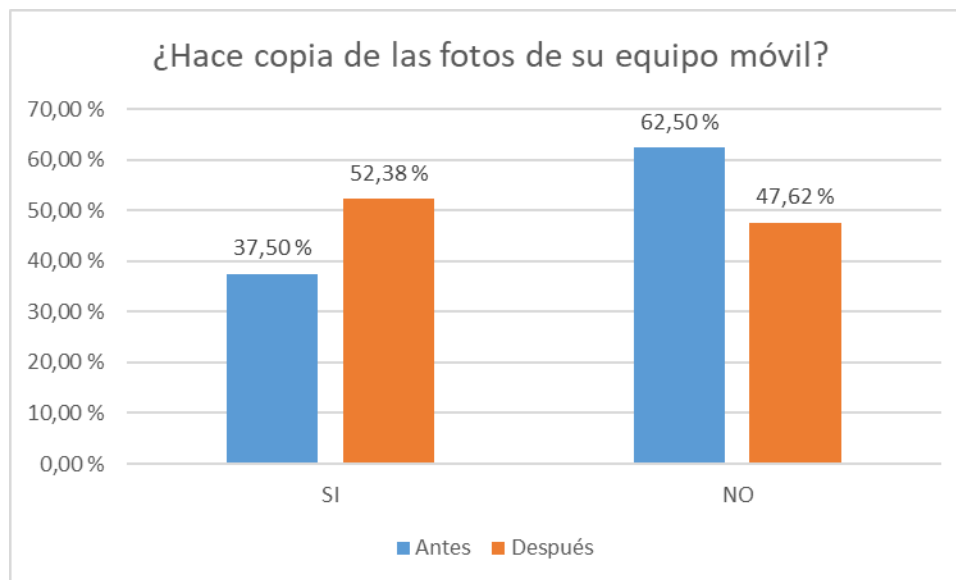
ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
20.	¿Tiene instalado software antivirus en su equipo móvil?	Si (35,12) No (64,88)	El 64,88% de los estudiantes no hace uso de un sistema de protección ante ataques de virus en el equipo móvil



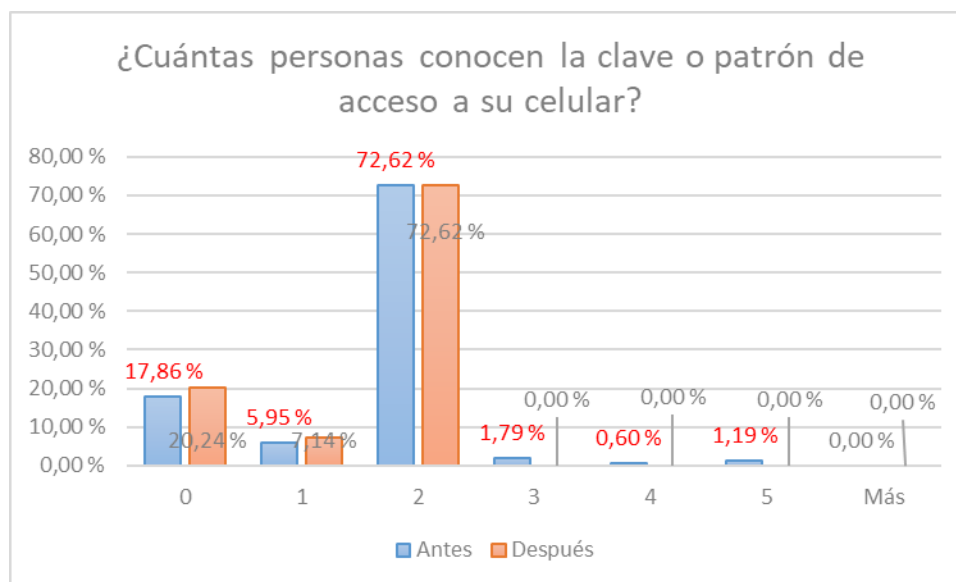
21.	¿Hace copia de la lista de contactos de su equipo móvil?	Si (36,90) No (63,10)	El 63,10% de los estudiantes están expuestos a pérdida o daño de los contactos de su dispositivo móvil.
-----	--	--------------------------	---



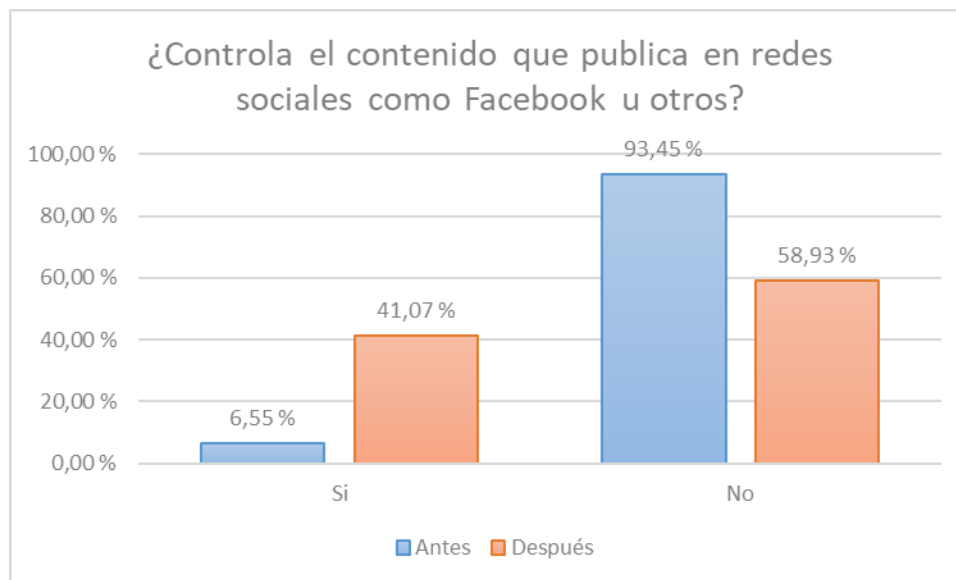
ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
22.	¿Hace copia de las fotos de su equipo móvil?	Si (37,50) No (62,50)	El 62,50% de los estudiantes están expuestos a pérdida o daño del contenido fotográfico de su dispositivo móvil.



ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
23.	¿Cuántas personas conocen la clave o patrón de acceso a su celular?	Cero (17,86) Una (5,95) Dos (72,62) Tres (1,79) Cuatro (0,60) Cinco (1,19) O Más (0,00)	El 72,62% de los estudiantes manifiestan compartir el mecanismo de acceso con dos personas adicionales, mientras que solo el 17,86% consideran una mayor privacidad en el uso de su dispositivo



ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
24.	¿Controla el contenido que publica en redes sociales como Facebook u otros?	Si (6,55) No (93,45)	El 93,45% de los estudiantes no está al tanto de los incidentes que pueden generarse al no controlar el público que sigue su perfil en las diferentes redes sociales, exponiéndose a delitos por parte de terceros.



ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS									
25.	¿Utiliza para conectarse a Internet redes públicas abiertas?	Si (76,19) No (23,81)	El 76,19% de los estudiantes están expuestos a robo, daño o espionaje de la información que fluye a través de los puntos de acceso públicos a internet									
<div><p>¿Utiliza para conectarse a Internet redes públicas abiertas?</p><table><thead><tr><th>Respuesta</th><th>Antes (%)</th><th>Después (%)</th></tr></thead><tbody><tr><td>Si</td><td>76,19</td><td>58,33</td></tr><tr><td>No</td><td>23,81</td><td>41,67</td></tr></tbody></table></div>				Respuesta	Antes (%)	Después (%)	Si	76,19	58,33	No	23,81	41,67
Respuesta	Antes (%)	Después (%)										
Si	76,19	58,33										
No	23,81	41,67										
26.	¿Le han pedido algún tipo de retribución o pago a cambio de no publicar o difundir información personal?	Si (4,76) No (95,24)	El 4,76% de los estudiantes han sido víctimas de algún tipo de delito generado por la información que publica de manera personal en las redes sociales o a través de aplicaciones del equipo móvil									
27.	¿Tiene alguna observación?	Si (2,98) No (97,02)	El 2,98% de los estudiantes manifiesta haber sido víctima de matoneo a raíz de información publicada a través de diferentes aplicaciones									

Fuente. Inédita

Luego de implementada la herramienta definida para disminuir los resultados obtenidos en la primera encuesta mediante charlas sobre seguridad informática, se realiza nuevamente el sondeo a través de la aplicación de la misma encuesta (Ver TABULACIÓN SEGUNDA ENCUESTA

Tabla 6) para determinar una posible variación en los resultados inicialmente obtenido, obtenido como resultado los siguientes valores.



## 10.2. TABULACIÓN SEGUNDA ENCUESTA

Tabla 6. Tabulación final encuesta aplicada

ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
1.	¿Cuenta con teléfono móvil?	Si (87,50) No (12,50)	Se mantuvo el número de equipos por estudiante durante el estudio.
2.	¿Qué tipo de teléfono móvil tiene?	Básico (4,76) Smartphone (79,17) Tablet con Simcard (3,57) No (12,50)	Se mantuvo la distribución de equipos por estudiante durante el estudio.
3.	¿Instala las actualizaciones disponibles del equipo celular (App y sistema operativo)?	Si ( <b>55,36</b> ) No ( <b>44,64</b> )	Se evidencia un cambio favorable sobre el "Si" de un <b>45,24%</b> con relación a la primera encuesta (10,12%) donde el estudiante se concientiza de la importancia de las actualizaciones de seguridad de sus equipos móviles.
4.	¿Tiene conexión a Internet constante?	Wifi (22,62) Plan (63,10) No (14,29)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
5.	¿Cuenta con plan de datos?	Prepago (31,55) Postpago (49,40) No (19,05)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
6.	¿Cuenta con plan de voz?	Prepago (32,74) Postpago (50,00) No (17,26)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
7.	¿Utiliza el equipo dentro del salón mientras está en clases?	Si (51,19) No (48,81)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
8.	¿Con qué frecuencia hace uso del equipo móvil?	Siempre (0,00) Muchas veces (73,21) Con frecuencia (7,74) A veces (1,79) Alguna vez (0,00) Nunca (17,26)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
9.	¿Qué uso le da al equipo móvil?	Redes sociales (82,74) Fotografía (87,50) Consultas (82,74) Reproductor (82,74) Video (82,74) Radio (5,36) Juegos (82,74)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
10.	¿Qué tipo de contenido consume en internet?	Humor (80,95) Sexual ( <b>57,74</b> ) Académico (82,74) Afectivo (82,74) Cultura Gral (78,57)	Se presenta una disminución del <b>16,07%</b> en cuanto al consumo de contenido sexual a través de internet con relación a la primera encuesta (73,81%) aplicada. Que se traduce en una disminución de la exposición del equipo móvil

ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
			a infecciones o robo de información generadas por este tipo de sitios web
11.	¿Qué red social consulta con más frecuencia con su equipo celular?	Facebook (63,69) Twitter (16,67) Google + (2,38) No (17,26)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
12.	¿Instala software por fuera de la Play store, y App Store?	Si (35,12) No (64,88)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
13.	¿Tiene implementado mecanismo de seguridad para acceder a su equipo?	Patrón <b>(73,21)</b> Huella (2,38) Facial <b>(2,98)</b> Números (1,19) No tiene <b>(11,90)</b> No aplica (8,33)	Se evidencia una mejoría en la implementación de mecanismos de seguridad en un <b>8,33%</b> en el uso del mecanismo de acceso de "Patrón" frente al (64,88%) que tenía inicialmente, así como un aumento del <b>1,79%</b> frente al (1,19%) en el uso de reconocimiento facial.
14.	¿Qué grado de dificultad tiene el mecanismo de seguridad configurado en su celular?	Alto <b>(16,07)</b> Medio <b>(15,48)</b> Bajo <b>(38,10)</b> No tiene (30,36)	Se evidencia una mejora en el grado de dificultad en el mecanismo de seguridad que tenían los estudiantes del <b>11,90%</b> con relación al (4,17%) del nivel "Alto", y un <b>7,14%</b> del nivel "medio" con relación al (8,33%) que tenía inicialmente.
15.	¿Comparte fotografías con personas que no conoce personalmente?	Si <b>(54,17)</b> No <b>(45,83)</b>	Se evidencia una mejoría en la disminución de la práctica de compartir contenido con personas desconocidas en un <b>15,48%</b> con relación al "Si" en un (69,64%)
16.	¿Comparte imágenes privadas a otra persona?	Si <b>(44,05)</b> No <b>(55,95)</b>	Se evidencia una mejoría en la disminución de la práctica de compartir contenido privado con personas en un <b>17,86%</b> con relación al "Si" en un (61,90%)
17.	¿A compartido imágenes privadas de tipo sexual a otra persona?	Si <b>(4,17)</b> No <b>(95,83)</b>	Se evidencia una mejoría en la disminución de la práctica de compartir contenido de tipo sexual en un <b>2,98%</b> con relación al "Si" en un (7,14%)
18.	¿Qué tan importante le resulta saber, lo que hagan otros con la información compartida de su parte?	Mucho (1,79) Algo <b>(47,02)</b> Poco <b>(32,14)</b> Nada (0,00) No lo había pensado <b>(1,79)</b> No (17,26)	Se logra un cambio en la percepción de los estudiantes del <b>47,02%</b> que consideran en "Algo" la seguridad de su información que comparte frente al (0,00%) inicialmente reportado.
19.	¿Su equipo celular ha sido infectado por virus?	Si (35,12) No (64,88)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.

ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
20.	¿Tiene instalado software antivirus en su equipo móvil?	Si ( <b>63,10</b> ) No ( <b>36,90</b> )	Mejora la protección del equipo móvil en un <b>27,98%</b> a partir del (35,12%) reportado inicialmente
21.	¿Hace copia de la lista de contactos de su equipo móvil?	Si ( <b>54,17</b> ) No ( <b>45,83</b> )	Mejora la protección de los datos ante la pérdida de los contactos en un <b>17,26%</b> a partir de los (36,90%) reportados inicialmente.
22.	¿Hace copia de las fotos de su equipo móvil?	Si ( <b>52,38</b> ) No ( <b>47,62</b> )	Se evidencia una mejoría en la protección ante pérdida o daño de contenido fotográfico del estudiante en un <b>14,88%</b> a partir del (37,50%) reportado inicialmente
23.	¿Cuántas personas conocen la clave o patrón de acceso a su celular?	Cero ( <b>20,24</b> ) Una ( <b>7,14</b> ) Dos (72,62) Tres ( <b>0,00</b> ) Cuatro ( <b>0,00</b> ) Cinco ( <b>0,00</b> ) O Más (0,00)	Se evidencia un cambio de conciencia entre los estudiantes reduciendo el número de personas que pueden entrar a sus equipos móviles limitando a máximo 2 personas. Para ello incrementan en un <b>2,38%</b> la limitación a “ <i>solo un usuario, es quien conoce el mecanismo de acceso</i> ” frente al (17,86%) inicialmente reportado, y en un <b>1,19%</b> al número de personas adicionales que conoce el mecanismo de acceso frente al (5,95%) inicialmente reportado
24.	¿Controla el contenido que publica en redes sociales como Facebook u otros?	Si ( <b>41,07</b> ) No ( <b>58,93</b> )	Se evidencia un cambio favorable de percepción de un <b>34,52%</b> en el control del contenido publicado frente al (93,45%) de estudiante que NO lo hacían.
25.	¿Utiliza para conectarse a Internet redes públicas abiertas?	Si ( <b>58,33</b> ) No ( <b>41,67</b> )	Se evidencia una disminución del <b>17,86%</b> en las conexiones a redes públicas frente al (23.81%) inicialmente reportado
26.	¿Le han pedido algún tipo de retribución o pago a cambio de no publicar o difundir información personal?	Si (4,76) No (95,24)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
27.	¿Tiene alguna observación?	Si (2,98) No (97,02)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.

Fuente. Inédita

## 11. CONCLUSIONES

Luego de implementadas las herramientas establecidas para el desarrollo del presente proyecto se llega a las siguientes conclusiones de acuerdo con la muestra analizada:

- A pesar de que un número considerable de estudiantes pertenecen al estrato socio-económico 2, la capacidad de adquisición de equipos móviles de comunicación con capacidad de conexión a internet y redes sociales es “Alta”, por lo que se deduce que la necesidad de estar conectado a la Internet y sus servicios no depende directamente de esta variable.
- El estudio indica, que los estudiantes gran parte del tiempo suelen hacer uso de sus equipos móviles sin que sea una limitante la jornada estudiantil. Lo que se puede traducir en un mal hábito y desarrollo de malas prácticas que podrían disminuir el rendimiento académico de los estudiantes.
- A pesar de que los dispositivos móviles son una herramienta para obtener conocimiento, gran parte de los encuestados utilizan este medio para interrelacionarse con otros, a través de conversaciones y publicaciones de material fotográfico que expone el nivel de seguridad de los encuestados.
- El amplio uso de las redes sociales, abre la posibilidad de que terceros obtengan bastante información sobre hábitos, gustos, tendencias, familias y localizaciones de los integrantes de la muestra.
- Los estudiantes se les concientiza a través de la charla proporcionada, sobre la implicación que puede traer la distribución y alcance incontrolado de material fotográfico expuesto en la Internet.
- Se logra concientizar con la ayuda de los folletos distribuidos y socializados, gran parte de la población encuestada, en la adopción y mejora de las prácticas de seguridad que permitan prevenir incidentes y delitos contra su persona o la de su círculo social/familiar.
- Los estudiantes de la muestra, de acuerdo con los resultados de las encuestas aplicadas, son conscientes de la importancia y beneficios que les resulta el mantener sus equipos actualizados y con software de protección como antivirus, que les ayuda a proteger sus datos personales ante intereses de terceros.
- Se socializa entre la población, los canales de comunicación disponibles en caso de ser víctimas de delitos informáticos como son: sitio web de la policía ([https://adenunciar.policia.gov.co/adenunciar/frm\\_denuncia\\_di.aspx](https://adenunciar.policia.gov.co/adenunciar/frm_denuncia_di.aspx)), Centro Cibernético policial (<https://caivirtual.policia.gov.co/>) y línea de atención telefónica 123. Adicionalmente, se comparte enlaces sobre guías de seguridad generadas por la policía y el centro informático

([https://caivirtual.policia.gov.co/sites/default/files/guia\\_facebook.pdf](https://caivirtual.policia.gov.co/sites/default/files/guia_facebook.pdf) y  
[https://caivirtual.policia.gov.co/sites/default/files/guia\\_whatsapp.pdf](https://caivirtual.policia.gov.co/sites/default/files/guia_whatsapp.pdf))

- A nivel personal como conclusión puedo inferir que, el desarrollo de este proyecto me permitió reconocer que, aunque se aportó parte de trabajo en la solución de una problemática que está en crecimiento, es necesario ahondar en un mayor esfuerzo, a fin de impactar a un mayor número de jóvenes. Dónde se les brinde conocimiento y herramientas que, les permita desarrollar habilidades en seguridad frente a un medio mayormente tecnológico.

## **12. RECOMENDACIONES**

- Realizar estudio, sobre el impacto que tiene el uso excesivo de equipos móviles en el desarrollo social, psicológico, afectivo, escolar, entre otros.
- Se debería, en aras de proteger la salud mental y social de los estudiantes, implementar controles y/o limitaciones más eficientes en el uso de los equipos móviles dentro de los ambientes escolares, con el objetivo que tengan mayor concentración sobre el conocimiento impartido en clase.
- Realizar estudio sobre tendencia de adquisición de equipos móviles en las diferentes edades de los jóvenes.
- Continuar con actividades de divulgación y concientización a través de charlas e info-guías, sobre temas de seguridad informática y protección de datos personales, entre los diferentes grupos estudiantiles de la Institución Educativa Catumare.

### **13. DIFICULTADES**

- A pesar de que se realice, difusión y concientización de la población en temas de seguridad informática, son muchos los estudiantes que pasan por alto la información suministrada exponiéndose a convertirse en víctimas de delitos informáticos.
- La falta de disposición de algunos pocos docentes, para disponer de sus horas de cátedra.
- A nivel técnico, se presentó una gran dificultad a la hora de plantear tanto las preguntas de la encuesta, como la dirección en la cual obtener los resultados luego de la tabulación de las respuestas.

## 14. BIBLIOGRAFÍA

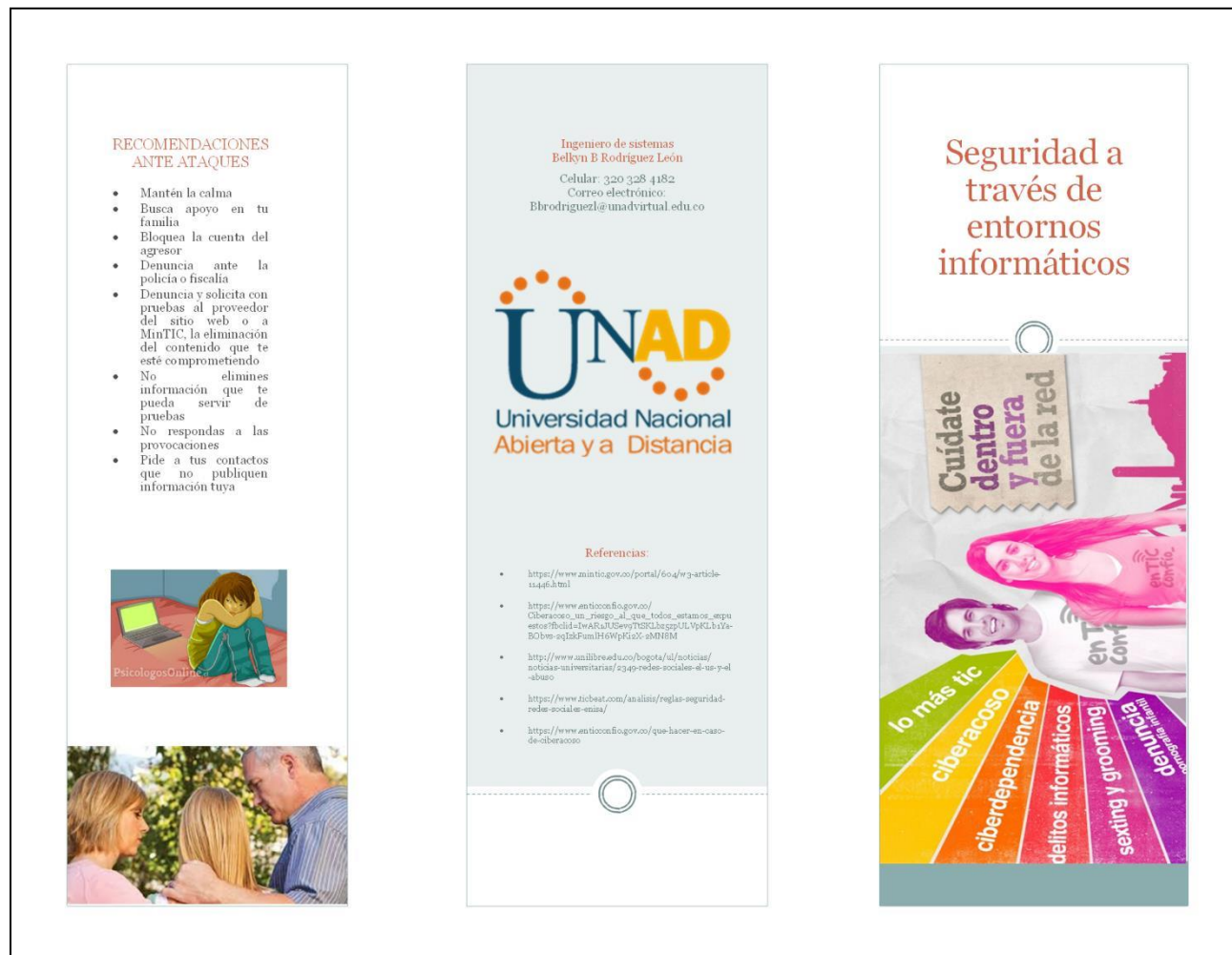
- Arias, F. G. (2012). El Proyecto de Investigación. Introducción a la Metodología Científica. 6ta. Edición. Caracas: Editorial Episteme, C.A.
- ANDALUCIA, Junta (2015). Internet Seguro. Disponible en: <http://www.juntadeandalucia.es/educacion/portals/delegate/content/68ec6247-5b4e-4879-a4e5-b61ff58f6b50>
- Baena, P. G. M. E. (2014). Metodología de la investigación. México: Larousse
- Benito, Carlos Andrés. Tendencias en investigación desarrollada por los estudiantes de enfermería de la primera y segunda cohorte del nuevo currículo de la Pontifica Universidad Javeriana en el periodo abril de 2008. Profesional en enfermería. Bogotá D.C. Pontifica Universidad Javeriana. 2008. 76 p. Disponible en <http://www.javeriana.edu.co/biblos/tesis/enfermeria/tesis08.pdf>. Consultado el 21 de septiembre de 2018.
- Grupo Editorial Patria. Páginas (38-69). Recuperado de <http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?docID=11038498>
- Cisneros, E. M. (2012). Cómo elaborar trabajos de grado (2a. ed.). Colombia: Ecoe Ediciones. Páginas (87-171) Recuperado de <http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?docID=10626100>
- Lerma, G. H. D. (2009). Metodología de la investigación: propuesta, anteproyecto y proyecto (4a ed.). Colombia: Ecoe Ediciones. Recuperado de <http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?docID=10552938>
- NTC 1486:2008. Documentación, Presentación de tesis, trabajos de grado y otros trabajos de investigación.
- NTC 5613:2008, Referencias bibliográficas. Contenido, forma y estructura.
- Sinnaps. (2018). Características del método cuantitativo. Disponible en <https://www.sinnaps.com/blog-gestion-proyectos/metodo-cuantitativo>. Consultado el 21 de septiembre de 2018.



## **ANEXOS**

## ANEXO A - FOLLETO

### Folleto, página 1





## Seguridad a través del uso de dispositivos móviles

En la actualidad, resulta indudable el uso de equipos móviles (celular) por todo tipo de personas en múltiples ámbitos de la vida, en especial por los jóvenes en donde se ve mayormente el incremento. Sin embargo, es necesario concientizar esta población sobre los alcances y riesgos a los que se exponen mientras hacen uso de sus equipos.

Ciertas prácticas que son llevadas de manera natural pueden, convertirse en serios problemas que podrían afectar su integridad física y emocional a nivel personal, familiar y/o social.

Por ello la importancia de transmitir este tipo de mensajes donde se pretende informar sobre los peligros a los que se exponen al hacer uso indebido de estos medios.

A continuación se exponen algunos peligros a los cuales deben estar atentos.

## PELIGROS EN EL USO DEL INTERNET



### Ciberacoso o cyberbullying

Agresión psicológica desde teléfonos celulares, Internet y juegos en línea. Se envían mensajes,

### Sexting:

Compartir contenidos eróticos o pornográficos

### Grooming:

Esgaño por parte de un adulto para comunicarse con menores de edad hasta ganarse su confianza y amistad, que en muchos casos termina en abuso sexual, introducción del menor a la pornografía y prostitución infantil.

### Phishing o fraude electrónico:

suplantación de la identidad por Internet. A través de redes sociales u otro medio, en donde el atacante perpetra sus fechorías.



### Ciberdependencia:

Adicción a los dispositivos digitales, o a permanecer conectado a Inter-



## REDES SOCIALES

Este servicio, resulta ser el canal de comunicación más utilizado por millones de personas a nivel mundial, para interactuar con otras personas a través de la creación de un perfil público.

Sin embargo, esta información que se comparte puede ser aprovechada por delincuentes para robarla, analizar tu comportamiento y hasta ubicar donde vives.

Su uso desmedido ha resultado en diversos peligros para la integridad de los afectados. Por ello es importante seguir las siguientes recomendaciones:

- Limite el acceso de terceros a tu perfil.
- Mantén tus datos personales de manera privada.
- Elige un Alias (Nombre a usar) diferente a tu nombre real.
- Evite usar información que permita identificarte y localizarte.
- No aceptes fácilmente solicitudes de desconocidos.
- Evalúa el contenido que publicas (fotos, comentarios, etc) evita publicar fotos comprometedoras.
- Deshabilita el geotiquetado en la información publicada.
- Utiliza una clave fuerte para el acceso a tu cuenta.
- No dejar desatendido su teléfono celular.
- Haz uso del sentido común.

## ANEXO B - MEMOFICHAS

<p><b>Nunca responder a ninguna solicitud de datos personales usando el correo electrónico, los sms o las llamadas telefónicas. Las entidades u organismos nunca solicitan esta información por estos medios.</b></p>	<p><b>Acordar un horario concreto y moderado de conexión a Internet.</b></p>
<p><b>Ellos ya tienen tus datos y, en todo caso, es la persona usuaria quien puede llamar para solicitarlos en caso de olvido o pérdida. Pero no al revés. Es cuestión de sentido común.</b></p>	<p><b>Diversificar las actividades cotidianas tratando de dedicarle a cada una el tiempo necesario.</b></p>
<p><b>Desconfiar de la dirección de sitio web o página contenida en un mensaje sospechoso.</b></p> <p><b>Normalmente se parecen a la dirección original del banco o entidad que dicen ser, pero no es igual.</b></p>	<p><b>Concretar las tareas a realizar en Internet antes de conectarse y tratar de mantener la atención en ellas hasta su terminación.</b></p>
<p><b>Asegurarse de que el acceso a la gestión de bancos por Internet se hace en una página de navegación segura HTTPS://. Este sistema exige que la entidad bancaria disponga de un certificado de seguridad y cifrado seguro que garantiza su autenticidad al cliente.</b></p>	<p><b>Cultivar a diario las relaciones personales y familiares.</b></p>

<p><b>Evita el envío de fotos comprometidas a tu pareja. El afecto puede demostrarse de otras formas. Piensa que puede utilizarla de forma no adecuada cuando vuestra relación haya terminado.</b></p>	<p><b>Respetar las horas de comida, sueño y descanso.</b></p>
<p><b>Reflexiona sobre las posibles consecuencias derivadas del envío de una foto personal comprometida a cualquier otra persona, sea conocida o no.</b></p>	<p><b>Moderar el uso de vídeo-juegos en la red.</b></p>
<p><b>No conectar a tu ordenador un pendrive o memoria USB que consideres infectada con algún virus.</b></p>	<p><b>Utilizar Internet para otras tareas más interesantes.</b></p>
<p><b>Mantener al día las actualizaciones del sistema operativo.</b></p>	<p><b>Dedicar el tiempo necesario al estudio y tareas escolares.</b></p>

<p><b>No utilizar software "pirata" de dudosa procedencia.</b></p>	<p><b>Hablar con mayores y profesorado.</b></p>
<p><b>Asegurarse de que está activo el firewall del sistema operativo para filtrar el tráfico del equipo con Internet.</b></p>	<p><b>Pueden ayudarte a organizar tu tiempo. Si consideras que te acosan, conserva las pruebas: emails, capturas de pantalla, etc.</b></p>
<p><b>No abrir emails ni archivos adjuntos que procedan de una persona desconocida.</b></p>	<p><b>Quien abusa, está cometiendo un delito.</b></p>
<p><b>Instalar en el equipo un buen programa antivirus y mantenerlo siempre actualizado.</b></p>	<p><b>Lo que se hace en Internet también tiene consecuencias.</b></p>

<p><b>Revisar con atención los documentos descargados y no permitir la ejecución de macros internas al abrirlos.</b></p>	<p><b>Si recibes amenazas graves, solicita ayuda con urgencia.</b></p>
<p><b>Cuando se sospeche de la existencia de una infección, actualizar el programa antivirus y escanear todas las unidades de disco.</b></p>	<p><b>Si te molestan de forma intencionada y reiterada, pide ayuda a tus mayores o al profesorado.</b></p>
<p><b>Si alguien se hace pasar por ti creando una cuenta similar a la tuya, denúncialo.</b></p>	<p><b>Trata de ignorar las provocaciones.</b></p>
<p><b>Cambia rápidamente la contraseña de acceso, si sospechas que está siendo utilizada.</b></p>	<p><b>Menos horas de sueño y comida: se prolonga la conexión a Internet por las noches, en lugar de dedicarlas a dormir, o incluso comer un bocadillo delante de la pantalla para no perder tiempo.</b></p>

<p><b>Si ya no puedes entrar porque te han cambiado la contraseña, denúncialo a tus mayores o al profesorado.</b></p>	<p><b>Creación de distintas identidades: se accede a un foro o chat con distintas identidades o personalidades. Síndrome de abstinencia: muestra malhumor y nerviosismo cuando no se puede conectar como consecuencia de un "castigo" o una avería.</b></p>
<p><b>Trata de reparar y explicar a las personas afectadas lo que han realizado en tu nombre.</b></p>	<p><b>Adaptación al estímulo: con el tiempo se buscan cada vez contenidos más estimulantes para alcanzar el mismo efecto.</b></p>
<p><b>Revisar el equipo con un programa anti-malware.</b></p>	<p><b>Conexión compulsiva: se siente la necesidad de conectarse muchas veces al día, aunque sea durante un corto periodo de tiempo. Esto se suele traducir en no dedicarle tiempo suficiente a otras tareas: deberes, aseo personal, cuidado, comida, vida familiar, etc.</b></p>
<p><b>Buscar y guardar las pruebas del chantaje: capturas de pantalla, conversaciones, mensajes, etc.</b></p>	<p><b>Búsqueda de satisfacción: se buscan constantemente contenidos relacionados con ciertos gustos o adicciones (juegos, temáticas, etc.)</b></p>




<b>Pedir siempre ayuda a tus mayores o profesorado.</b>	<b>Dispersión de la atención: se plantean varias tareas a la vez sin centrar la atención ni terminar ninguna de ellas.</b>
<b>Aumentar las opciones de privacidad de tu perfil en las redes sociales.</b>	<b>Pérdida de la noción del tiempo: se conecta para una tarea determinada, pero se termina dedicándole mucho más tiempo.</b>
<b>No ceder al chantaje en ningún caso.</b>	<b>Acordar un horario concreto y moderado de conexión a Internet.</b>
<b>Modificar todas las contraseñas de acceso.</b>	<b>Concretar las tareas a realizar en Internet antes de conectarse y tratar de mantener la atención en ellas hasta su terminación.</b>

<b>Mantener la privacidad de las imágenes e informaciones personales.</b>	<b>Moderar el uso de videojuegos en la red.</b>
<b>No dar las contraseñas del equipo a nadie para evitar el robo de información.</b>	<b>Utilizar Internet para otras tareas más interesantes.</b>
<b>No proporcionar imágenes, vídeos o informaciones personales a personas desconocidas.</b>	<b>Es importante hablar con los mayores y el profesorado. Te pueden ayudar a organizar tu tiempo.</b>
<b>Nunca comuniques a nadie tus contraseñas.</b>	<b>Diversificar tus actividades cotidianas tratando de dedicarle a cada una el tiempo necesario.</b>

<b>Evita que nadie te mire cuando introduzcas la contraseña.</b>	<b>Cultivar a diario las relaciones personales y familiares.</b>
<b>Utiliza contraseñas seguras, evitando aquellas cortas o triviales.</b>	<b>Respetar las horas de sueño y descanso, así como las comidas acompañado en familia.</b>
<b>En los ordenadores de uso público o del centro, recuerda cerrar la sesión.</b>	<b>Dedicar el tiempo necesario al estudio y tareas escolares.</b>
<b>No almacenes las contraseñas.</b>	

## ANEXO C – PRESENTACIÓN

**CEAD ACACIAS**



**EVALUACIÓN DEL NIVEL DE SEGURIDAD INFORMÁTICA EN EL USO DE DISPOSITIVOS MÓVILES EN LA COMUNIDAD ESTUDIANTIL DE LA INSTITUCIÓN EDUCATIVA CATUMARE DE LA CIUDAD DE VILLAVICENCIO PARA LOS GRADOS DE MEDIA BÁSICA 9, 10 Y 11**


**Ing. Belkyn Rodríguez**

Especialización en Seguridad Informática

**Seguridad al usar Internet**



**Peligros al usar Internet**



**Peligros en las redes sociales**



! Breve video donde nos exponen algunos peligros que acechan en las redes sociales (Facebook, Twitter, etc)

**Redes Sociales**



! Potencialidad Vs desaprovechamiento

**Peligros en las redes sociales**



! Invitaciones de desconocidos con nombre falsos  
Solicitud de información personal y de localización

## Quiénes nos protegen

- Bienestar familiar
- Comisaria de familia
- Policía Nacional
- Fiscalía





LEYES QUE PROTEGEN A LOS NIÑOS, NIÑAS Y ADOLESCENTES EN COLOMBIA

**!** No sature de información o texto las diapositivas, trate de sintetizar al máximo y no copie y pegue textos completos de otros documentos.

## Recomendaciones de seguridad

- Limite el acceso de terceros a tu perfil.
- Mantén tus datos personales de manera privada
- Elige un Alias (Nombre a usar) diferente a tu nombre real
- Evite usar información que permita identificarte y localizarte
- No aceptes fácilmente solicitudes de desconocidos
- Evalúa el contenido que publicas (fotos, comentarios, etc) evita publicar fotos comprometedoras
- Deshabilita el geoetiquetado en la información publicada
- Utiliza una clave fuerte para el acceso a tu cuenta
- No dejar desatendido su teléfono celular
- Haz uso del sentido común

# GRACIAS POR SU ATENCIÓN

## ANEXO D - FORMATO DE ASISTENCIA

### FORMATO DE ASISTENCIA

**OBJETIVO:** Orientar a estudiantes de los grados 9, 10 y 11 de la Institución Educativa Catumare de la ciudad de Villavicencio sobre seguridad a través de dispositivos móviles

FECHA:	Sept 14 de 2018		SEDE:	campesino		
ID	NOMBRES Y APELLIDOS ASISTENTE			GRADO	CURSO	JORNADA
1	Astrid Yovana Estrada			10	2	T
2	Nancy Matela Caba			10	2	T
3	Adriana Yisel Bejarano Jofet.			10	2	T
4	Nelson Céspedes Alvarez			10	II	T
5	Sandra Benito Guevara.			10	2	T
6	Edmundo Bonilla Garcia.			10	2	T
7	Sandra S. Naranjo			10	2	T
8	Hury Jonathan Rodriguez Jrc			10	2	T
9	Victor Manuel Pardo			10	2	T
10	LEIDY CAROL DEJA BARRERA			10	2	T
11	Junior Andres Alvarez Botos			10	2	T
12	Jonathan Cubillos.			10	2	T
13	Diana Gisela Tauta Alzate			10	2	T
14	Humar Eduardo Montano Parrado			10	2	T
15	Esneider Valderrama			10	2	T

  
 FIRMA CAPACITADOR

# FORMATO DE ASISTENCIA

OBJETIVO: Orientar a estudiantes de los grados 9, 10 y 11 de la Institución Educativa Catumare de la ciudad de Villavicencio sobre seguridad a través de dispositivos móviles

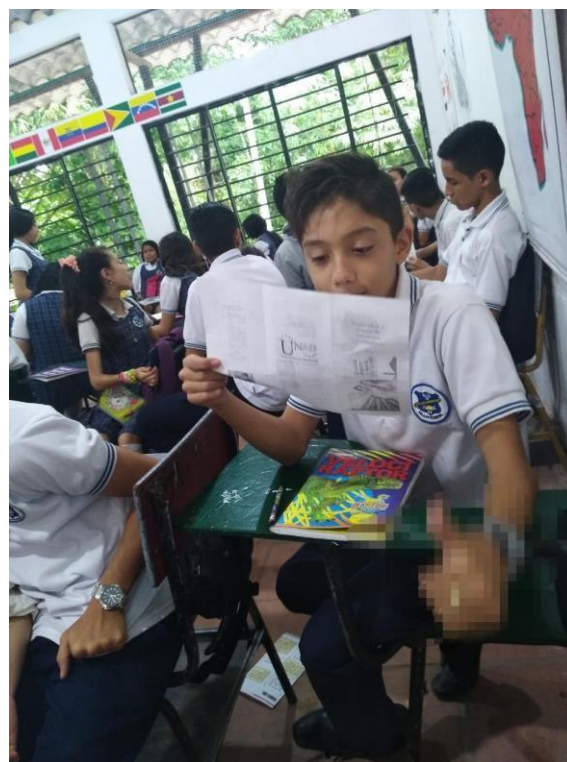
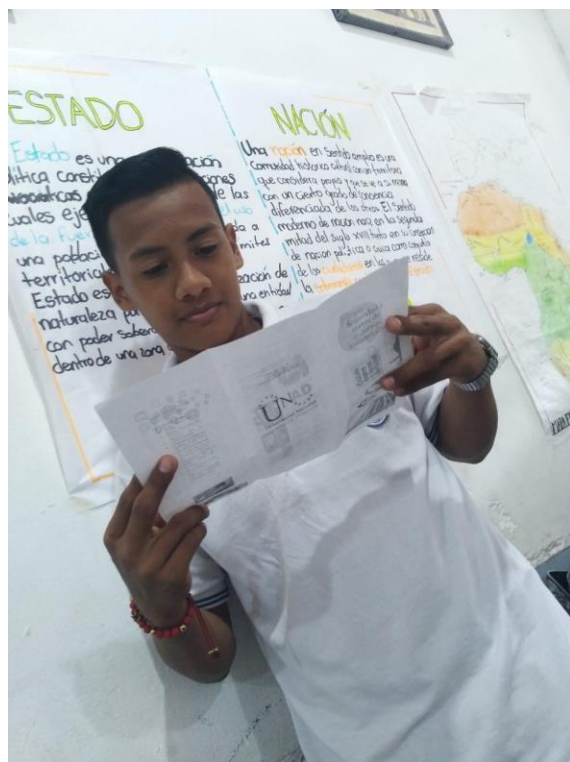
FECHA:	SEDE:		CURSO		JORNADA
septiembre 06 2018	Principal				
ID	NOMBRES Y APELLIDOS ASISTENTE		GRADO	CURSO	JORNADA
1	Ana Silvia Bizarro Domínguez		9	1	M
2	Jhon Carlos Herrera		9	1	M
3	Algodora Myleny Arevalo Gómez		9	1	M
4	Jordi Paez		9	1	M
5	Jairo Alexander Acall Rodríguez		9	1	M
6	Mariluz Vargas Acuña		9	1	M
7	YONATAN GARCÍA VARGAS		9	1	M
8	Jiroth Alexander Sierra Jimenez		9	1	M
9	YENICA ROSA SOTA BERNARDO		9	1	M
10	JHAN Lindares Correa		9	1	M
11	William García Tique		9	1	M
12	Yhanna Idaly Zoto		9	1	M
13	Juliana Arias		9	2	M
14	Teresal Garavito Burgos		9	2	M
15	Angie Natalia Reyes		9	2	M

*Belkynh*

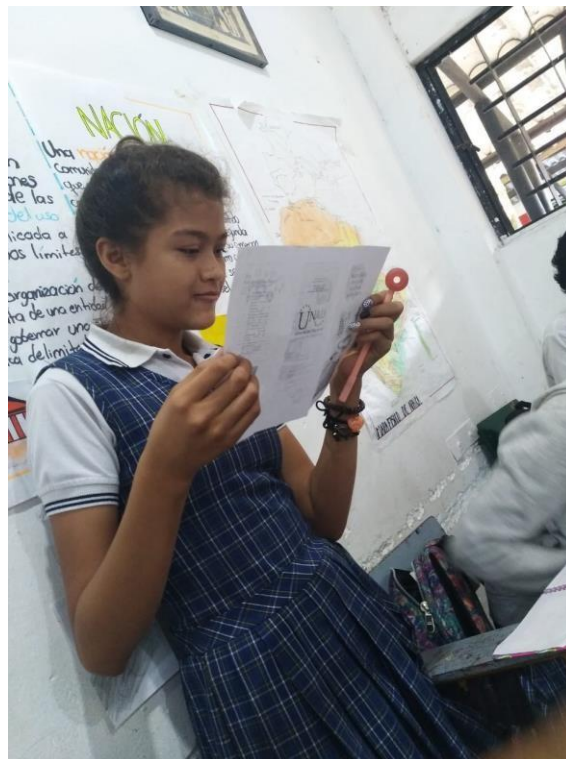
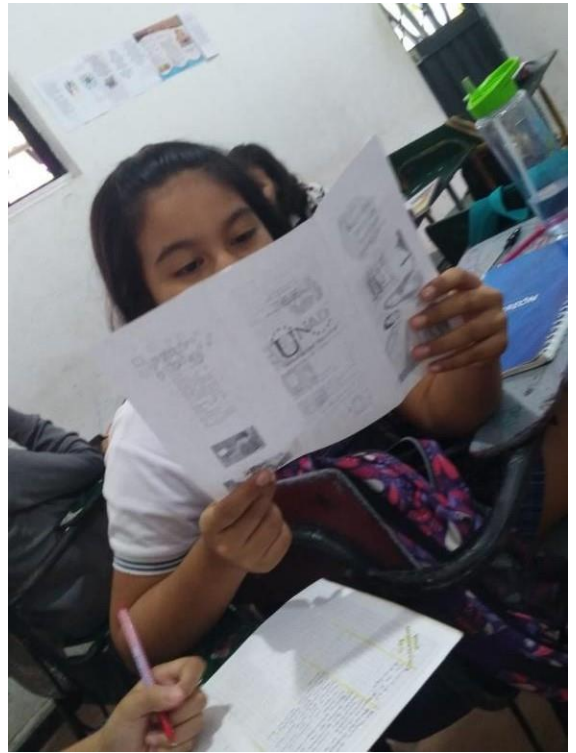
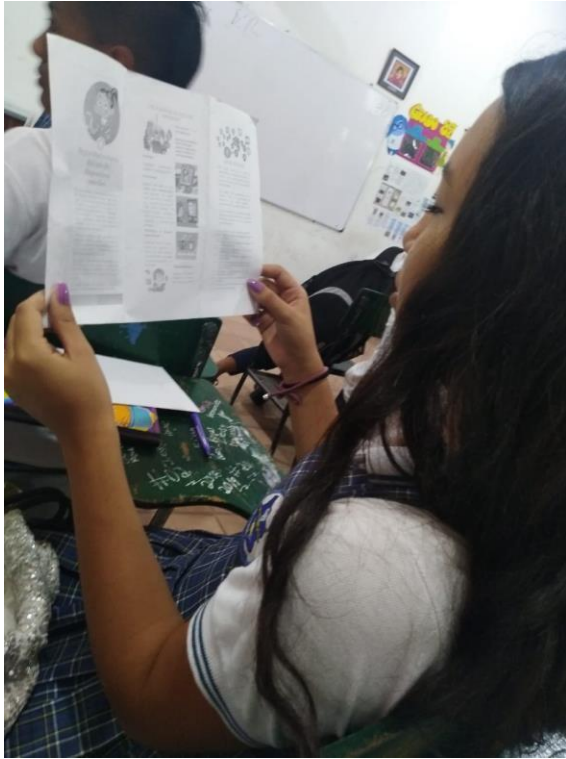
FIRMA CAPACITADOR



## ANEXO E - GALERIA FOTOGRÁFICA







## ANEXO F - ENCUESTA INICIAL APLICADA

CARACTERIZACIÓN ENCUESTADO									
Grado/Curso		Edad		Sexo		Estrato Social			
9-3		15		M		2			
IDENTIFICACIÓN EQUIPO MÓVIL									
ID	PREGUNTAS								
1.	¿Cuenta con teléfono móvil?								
2.	¿Qué tipo de teléfono móvil tiene?								
3.	¿Instala las actualizaciones disponibles del equipo celular (App y sistema operativo)?								
CONECTIVIDAD									
4.	¿Tiene conexión a Internet constante?								
5.	¿Cuenta con plan de datos?								
6.	¿Cuenta con plan de voz?								
USO									
7.	¿Utiliza el equipo dentro del salón mientras está en clases?								
8.	¿Con qué frecuencia hace uso del equipo móvil?								
9.	¿Qué uso le da al equipo móvil?								
10.	¿Qué tipo de contenido consume en internet?								
11.	¿Qué red social consulta con más frecuencia con su equipo celular?								
12.	¿Instala software por fuera de la Play store, y App Store?								
13.	¿Tiene implementado mecanismo de seguridad para acceder a su equipo?								
14.	¿Qué grado de dificultad tiene el mecanismo de seguridad configurado en su celular?								
15.	¿Comparte fotografías con personas que no conoce personalmente?								
16.	¿Comparte imágenes privadas a otra persona?								
17.	¿A compartido imágenes privadas de tipo sexual a otra persona?								
18.	¿Qué tan importante le resulta saber, lo que hagan otros con la información compartida de su parte?								
19.	¿Su equipo celular ha sido infectado por virus?								
20.	¿Tiene instalado software antivirus en su equipo móvil?								
21.	¿Hace copia de la lista de contactos de su equipo móvil?								
22.	¿Hace copia de las fotos de su equipo móvil?								
23.	¿Cuántas personas conocen la clave o patrón de acceso a su celular?								
24.	¿Controla el contenido que publica en redes sociales como Facebook u otros?								
25.	¿Utiliza para conectarse a Internet redes públicas abiertas?								
26.	¿Le han pedido algún tipo de retribución o pago a cambio de no publicar o difundir información personal?								
27.	¿Tiene alguna observación?								

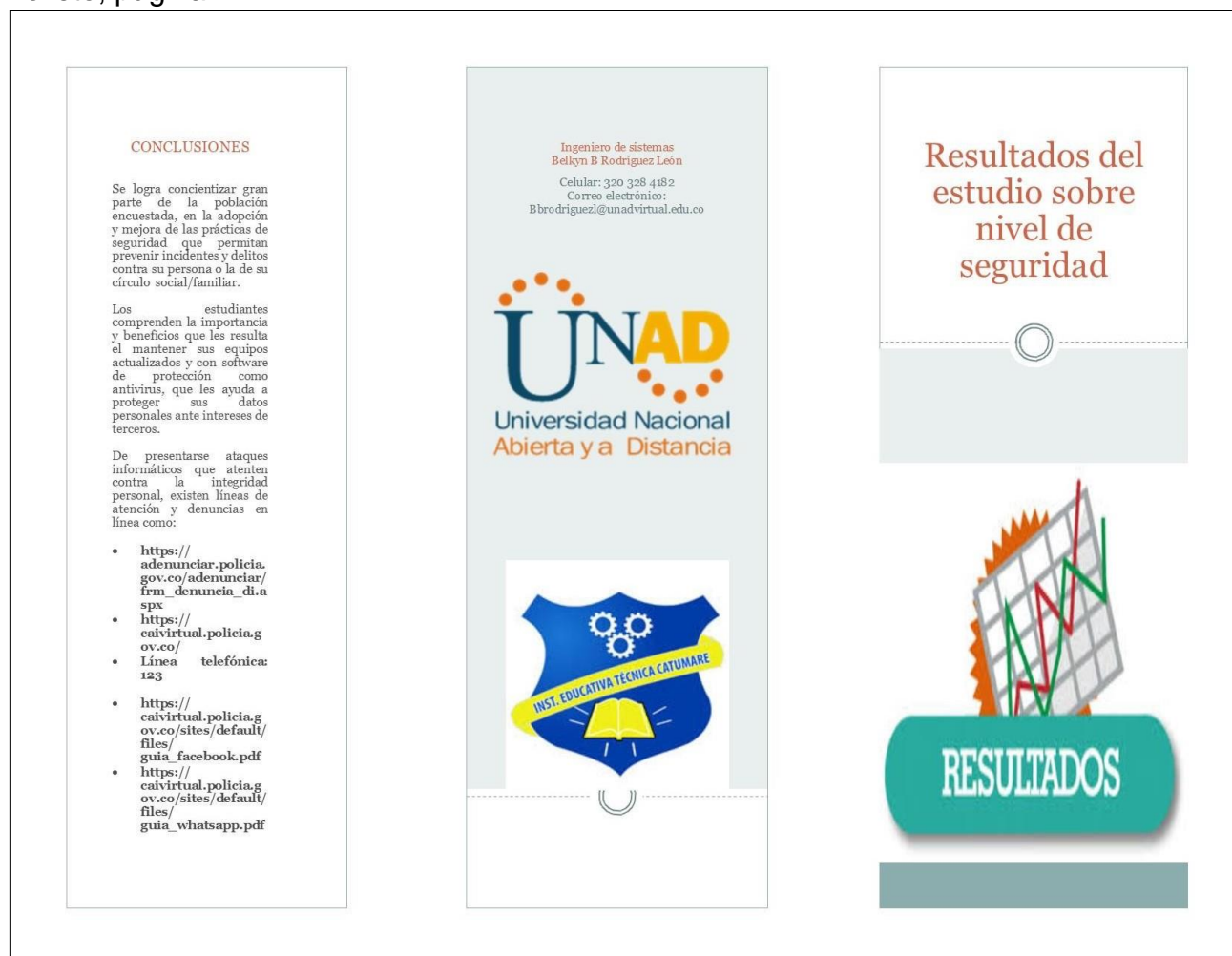


## ANEXO G - ENCUESTA FINAL APLICADA

CARACTERIZACIÓN ENCUESTADO									
Grado/Curso		Edad		Sexo		Estrato Social			
11 - 1		19		F		3			
IDENTIFICACIÓN EQUIPO MÓVIL									
ID	PREGUNTAS								
1.	¿Cuenta con teléfono móvil?			Si <input checked="" type="checkbox"/>			No		
2.	¿Qué tipo de teléfono móvil tiene?			Básico			Smartphone <input checked="" type="checkbox"/>		
3.	¿Instala las actualizaciones disponibles del equipo celular (App y sistema operativo)?			Si <input checked="" type="checkbox"/>			No		
CONECTIVIDAD									
4.	¿Tiene conexión a Internet constante?			Wifi			Plan de datos <input checked="" type="checkbox"/>		
5.	¿Cuenta con plan de datos?			Prepago			Postpago <input checked="" type="checkbox"/>		
6.	¿Cuenta con plan de voz?			Prepago			Postpago <input checked="" type="checkbox"/>		
USO									
7.	¿Utiliza el equipo dentro del salón mientras está en clases?			Si			No <input checked="" type="checkbox"/>		
8.	¿Con qué frecuencia hace uso del equipo móvil?			Siempre			Muchas veces <input checked="" type="checkbox"/>		
9.	¿Qué uso le da al equipo móvil?			Califique del 0 al 10, siendo "0" nada y "10" mucho					
	Uso de chat			8			Consulta de tareas o actividades		
	Cámara fotográfica			8			Reproductor de música		
				7			Cámara de video		
				4			Radio		
10.	¿Qué tipo de contenido consume en internet?			Humor <input checked="" type="checkbox"/>			Sexual <input checked="" type="checkbox"/>		
				Académico <input checked="" type="checkbox"/>			Afectivo <input checked="" type="checkbox"/>		
							Cultura gral		
11.	¿Qué red social consulta con más frecuencia con su equipo celular?			Facebook <input checked="" type="checkbox"/>			Twitter		
				Google +			Linkedin		
12.	¿Instala software por fuera de la Play store, y App Store?			Si <input checked="" type="checkbox"/>			¿Cuál sitio? <u>uptodowne</u>		
13.	¿Tiene implementado mecanismo de seguridad para acceder a su equipo?			Patrón <input checked="" type="checkbox"/>			Huella		
				Facial			Números		
							No tiene		
14.	¿Qué grado de dificultad tiene el mecanismo de seguridad configurado en su celular?			Alto			Medio <input checked="" type="checkbox"/>		
				Bajo			No tiene		
15.	¿Comparte fotografías con personas que no conoce personalmente?			Si			No <input checked="" type="checkbox"/>		
16.	¿Comparte imágenes privadas a otra persona?			Si <input checked="" type="checkbox"/>			No		
17.	¿A compartido imágenes privadas de tipo sexual a otra persona?			Si			No <input checked="" type="checkbox"/>		
18.	¿Qué tan importante le resulta saber, lo que hagan otros con la información compartida de su parte?			Mucho			Algo		
				Poco <input checked="" type="checkbox"/>			Nada		
							No lo había pensado		
19.	¿Su equipo celular ha sido infectado por virus?			Si <input checked="" type="checkbox"/>			No		
20.	¿Tiene instalado software antivirus en su equipo móvil?			Si <input checked="" type="checkbox"/>			No		
21.	¿Hace copia de la lista de contactos de su equipo móvil?			Si <input checked="" type="checkbox"/>			Cómo: <u>Google</u>		
22.	¿Hace copia de las fotos de su equipo móvil?			Si <input checked="" type="checkbox"/>			Cómo: <u>Google</u>		
23.	¿Cuántas personas conocen la clave o patrón de acceso a su celular?			0			1		
				2 <input checked="" type="checkbox"/>			3		
				4			5		
							Más		
24.	¿Controla el contenido que publica en redes sociales como Facebook u otros?			Si <input checked="" type="checkbox"/>			No		
25.	¿Utiliza para conectarse a Internet redes públicas abiertas?			Si			No <input checked="" type="checkbox"/>		
26.	¿Le han pedido algún tipo de retribución o pago a cambio de no publicar o difundir información personal?			Dinero			Artículos		
				Abuso personal			Abuso sexual		
							No <input checked="" type="checkbox"/>		
27.	¿Tiene alguna observación?			<u>NO</u>					

## ANEXO H – FOLLETO DE RESULTADOS

### Folleto, página 1



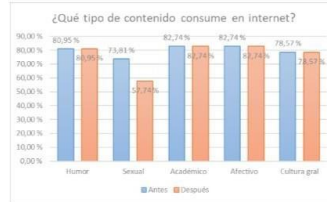


## Resultados

La implementación del proyecto que busca identificar el nivel de seguridad en el uso de dispositivos móviles en los grados 9, 10 y 11 de la Institución Educativa Catumare, permitió generar en la población vinculada a estos grupos interrogantes sobre la manera en que están compartiendo su información personal entre las diferentes herramientas y servicios disponibles en este medio.

A continuación, se exponen apartes de los resultados obtenidos de manera general

### Uso habitual del Internet



### Mecanismos de seguridad implementados



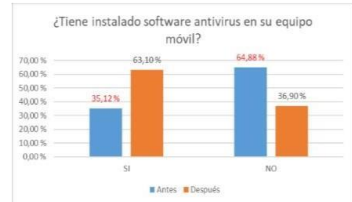
### Dificultad del mecanismos de seguridad



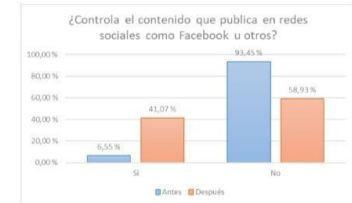
### Compartir información con desconocidos



### Uso de antivirus



### Control del contenido en redes



## **ANEXO I – INFORME EJECUTIVO**

### **INFORME EJECUTIVO**

Presento el siguiente informe en el que se describe el resultado del trabajo realizado en la Institución Educativa Catumare de la ciudad de Villavicencio, según lo acordado en reuniones preliminares.

### **OBJETIVO GENERAL**

Evaluar el nivel de las medidas de seguridad informática que implementan los estudiantes de los grados 9, 10 y 11 de la Institución Educativa Catumare de la ciudad de Villavicencio, al momento de hacer uso de dispositivos Smartphone para compartir información en redes sociales u otros medios de transferencia de información personal.

### **OBJETIVOS ESPECÍFICOS**

- Realizar reconocimiento de la Institución educativa, cómo está conformada, jornadas académicas, cantidad de estudiantes, y distribución de cursos.
- Elaborar plan de trabajo para socializarlo con el personal administrativo de la institución que incluya actividades, tareas, pruebas iniciales y finales, recursos necesarios, inconvenientes, responsables y tiempo de ejecución.
- Diseñar y ejecutar talleres de concientización, que permitan mejorar la cultura de la población en estudio, relacionados con el uso adecuado de las redes sociales y demás información personal a través de dispositivos móviles, permitiendo expandir este conocimiento al entorno social y familiar de los jóvenes.
- Fortalecer el conocimiento adquirido en el ámbito educativo y profesional, a través de charlas que permita generar un impacto positivo en las comunidades afectadas por el proyecto y que les permita tener la visión de nuevas estrategias a manejar por parte de los estudiantes de la institución educativa Catumare de la ciudad de Villavicencio.
- Generar y socializar entre las directivas de la institución y la población estudiantil de los grados 9, 10 y 11, informe con los resultados obtenidos, y sus respectivas recomendaciones para mitigar los riesgos y vulnerabilidades de seguridad identificadas.

## **ALCANCE**

La implementación de charlas de concientización sobre seguridad informática, en la Institución Educativa Catumare de la ciudad de Villavicencio, a las directivas de la institución y la población estudiantil de los grados 9, 10 y 11, con el objeto de permitir a la población afectada, reducir la brecha de exposición, a riesgos y/o peligros informáticos que comprometan su seguridad personal, familiar y/o social.

## **VARIABLES**

### **INDEPENDIENTES.**

Hace referencia a las charlas sobre seguridad informática en equipos móviles como celulares, a través de las cuales se busca evaluar el nivel de seguridad que aplican los estudiantes de los grados 9, 10 y 11 de la Institución Educativa.

### **DEPENDIENTES.**

Mejorar el nivel de seguridad informática, sobre equipos móviles de la población en estudio de la Institución Educativa Catumare.

## **METODOLOGÍA**

A continuación, se describe las fases de la metodología implementada, con las cuales se busca obtener los resultados de la investigación de campo.

### **PRELIMINAR.**

Realizar levantamiento de información sobre la Institución Educativa, relacionada con jornadas académicas, cantidad de estudiantes, y distribución de cursos.

Para desarrollar esta fase, se realizó reuniones con el personal administrativo y docentes, en donde se recopiló datos de la población estudiantil matriculada durante el presente año académico, con ello se determinó la muestra utilizada. Adicionalmente, se recopiló información relacionada con la conformación de la Institución Educativa Catumare relacionada con sedes, jornadas y cantidad de estudiantes.

### **PRINCIPALES ACTIVIDADES PLANEADAS A EJECUTAR**

El universo seleccionado, fue la totalidad de estudiantes matriculados en la Institución Educativa durante el 2018, distribuidos en las 6 sedes que corresponde a 2.032 alumnos.

La población evaluada fueron los 503 estudiantes, inscritos en los grados 9, 10 y 11 de la Institución Educativa.

La muestra representativa, con que se trabajó fue de 168 jóvenes (1/3 de la población), cuyas edades oscilan entre los 15 y 22 años, distribuidos entre los géneros masculinos y femeninos. Los candidatos seleccionados, aplicaron para las dos encuestas realizadas (Inicial y final).

De acuerdo con el cronograma de trabajo, se ejecutaron las siguientes actividades generales, las cuales fueron desarrolladas en el lapso comprendido entre agosto y diciembre de 2018:

Socialización del proyecto con coordinadores de las diferentes sedes, donde se expuso alcance, recursos, metodología de desarrollo basada en la aplicación de encuesta (al iniciar el proyecto y luego de realizada charla sobre seguridad), aplicación de charlas de concientización sobre seguridad informática a través de equipos móviles de estudiantes y tabulación de datos recopilados, en donde se presentó los resultados obtenidos.

Socialización con docentes de los grados noveno, décimo y undécimo de las diferentes sedes, donde se programó los espacios y horarios requeridos para cada actividad.

El desarrollo de las actividades definidas, se dividió en tres (3) secciones de trabajo con los diferentes grupos de estudiantes.

### ***Primera***

Charla introductoria con estudiantes de cada curso, con duración de 15 minutos sobre actividad a realizar.

Distribución, aplicación y posterior recolección de encuesta de percepción sobre prácticas personales de seguridad a través del uso de equipos móviles a cada estudiante del curso, con duración de 15 minutos.

Tabulación de datos recopilados en encuestas aplicadas (1 semana).

### ***Segunda***

Elaboración de charlas de concientización a la población incluida en el proyecto, sobre seguridad informática a través de los diferentes equipos de comunicación móvil del que hacen uso, cuyo objetivo es disminuir incidentes y peligros que se puedan presentar mediante este tipo de dispositivos, con duración de 45 minutos por grupo.

Estas charlas se realizaron en el auditorio y algunos salones en cada sede, contando con dispositivos de audio y proyección para tal fin.

### ***Tercera***

Charla introductoria con estudiantes de cada curso, con duración de 15 minutos sobre actividad a realizar.

Distribución de encuesta final, re-aplicación y recolección de formatos luego de aplicada la



encuesta de percepción, sobre prácticas personales de seguridad a través del uso de equipos móviles a cada estudiante, con duración de la actividad de 15 minutos.

Tabulación de datos recopilados en encuestas aplicadas (2 semanas).

Presentación de evidencias recopiladas (1 semana).

Generación de informe con resultados obtenidos (2 días).

Socialización de resultados con docentes, coordinadores y rectoría (2 horas).

## **ESQUEMA DE TRABAJO**

Se diseñó y ejecutó mecanismos de concientización, que permitieron mejorar la cultura de la población en estudio, relacionada con el uso de dispositivos móviles, redes sociales y demás información personal de los estudiantes de la Institución Educativa, permitiendo expandir este conocimiento al entorno social y familiar de los jóvenes.

Para el desarrollo de esta etapa, se diseñó un folleto en donde se manejó temas relacionados con seguridad y privacidad.

Se fortaleció el conocimiento adquirido en el ámbito educativo y profesional, a través de charlas que permiten generar un impacto positivo en las comunidades afectadas por el proyecto y que les permite tener la visión de nuevas estrategias a manejar por parte de los estudiantes de la Institución Educativa Catumare de la ciudad de Villavicencio.

Estas charlas, se realizaron con el objetivo de fortalecer la información distribuida mediante los folletos informativos. El contenido tratado contó con la aprobación de las directivas de la institución, y se hizo uso de herramientas tecnológicas como equipos de cómputo y videobeams, los cuales permitieron llegar a un mayor número de estudiantes por grupos.

## **FINALES.**

Se generó y socializó entre las directivas de la institución y la población estudiantil de los grados 9, 10 y 11, un informe con los resultados obtenidos.

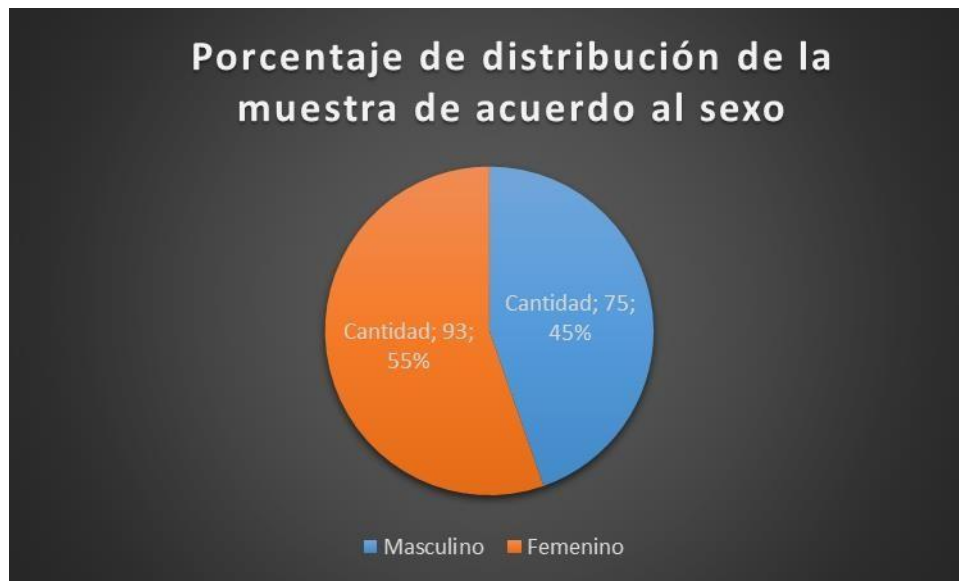
Para los estudiantes participantes en la muestra, se entregó un folleto informativo, en donde se presentó los resultados del estudio de manera general.

## RESULTADOS OBTENIDOS DE LA ENCUESTA

A continuación, se relacionan los resultados obtenidos luego de aplicada la encuesta de manera inicial y posteriormente, después de realizadas las charlas sobre seguridad informática.

Con relación a la caracterización de la población encuestada, el porcentaje de distribución de acuerdo al género, se da de acuerdo con la Figura 1.

Figura 1. Porcentaje de distribución de la muestra de acuerdo al sexo

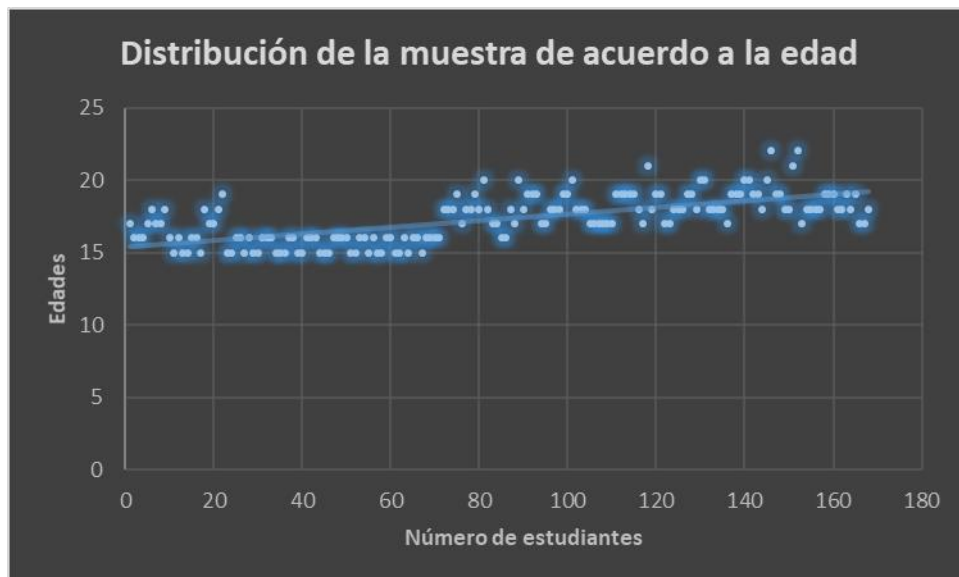


Fuente. Inédita

La Figura 1 muestra que la muestra seleccionada está conformada mayormente por estudiantes femeninas (55%), esto podría indicar que este tipo de población es más vulnerable a incidentes de seguridad informática debido a que están más en contacto con las redes sociales y divulgación de contenido visual como fotografías.

De acuerdo con la edad informada por los participantes de la muestra, se evidencia en la Figura 2.

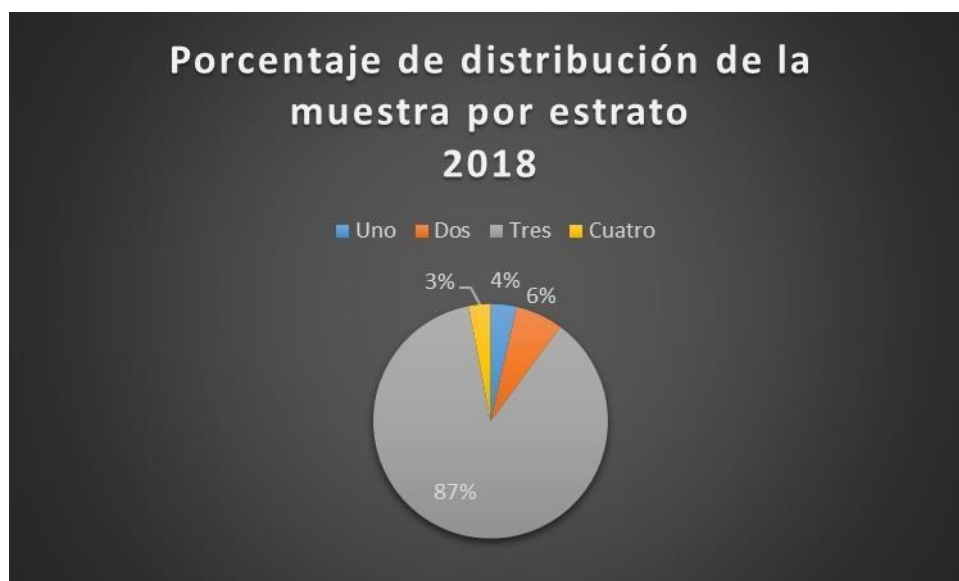
Figura 2. Distribución de la muestra de acuerdo a la edad



Fuente. Inédita

De acuerdo con el porcentaje de distribución de la población encuestada por estrato socio-económico, la mayoría de estudiantes son de estrato social 3.

Figura 3. Distribución de la muestra por estrato socio-económico



Fuente. Inédita

Tabla 1. Tabulación primera encuesta aplicada

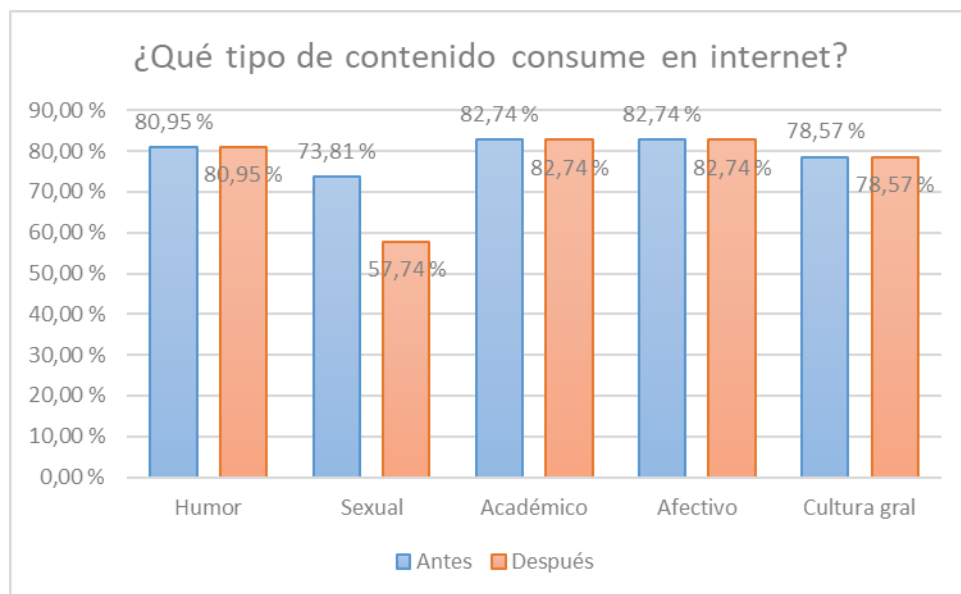
ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
28.	¿Cuenta con teléfono móvil?	Si (87,50) No (12,50)	El 87,50% de los estudiantes tienen celulares
29.	¿Qué tipo de teléfono móvil tiene?	Básico (4,76) Smartphone (79,17) Tablet con Simcard (3,57) No (12,50)	El 79,17% de los estudiantes cuentan con equipos Smartphone con capacidad de conexión a internet
30.	¿Instala las actualizaciones disponibles del equipo celular (App y sistema operativo)?	Si (10,12) No (89,88)	El 89,88% de estudiantes no realiza las actualizaciones del sistema, cuando el fabricante libera mejoras para el sistema operativo.

¿Instala las actualizaciones disponibles del equipo celular (App y sistema operativo)?

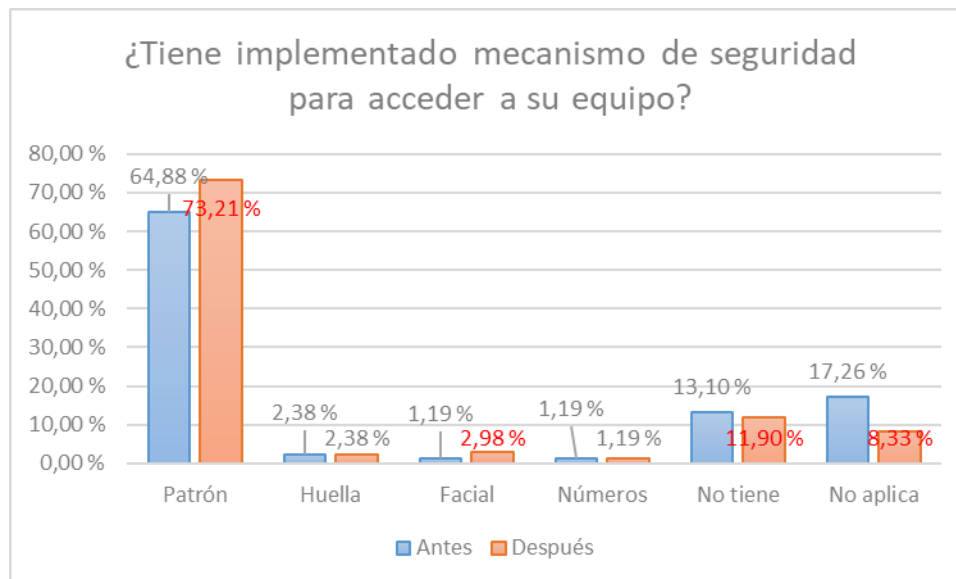
Respuesta	Antes (%)	Después (%)
SI	10,12 %	55,36 %
NO	89,88 %	44,64 %

31.	¿Tiene conexión a Internet constante?	Wifi (22,62) Plan (63,10) No (14,29)	El 63,10% de los estudiantes cuentan con un plan de datos (prepago o postpago) que les permite estar conectados a Internet y demás servicios
32.	¿Cuenta con plan de datos?	Prepago (31,55) Postpago (49,40) No (19,05)	El 49,40% de los estudiantes cuenta con planes postpago que les permite tener acceso constante a Internet
33.	¿Cuenta con plan de voz?	Prepago (32,74) Postpago (50,00) No (17,26)	El 50,00% de los estudiantes cuenta con plan de voz
34.	¿Utiliza el equipo dentro del salón mientras está en clases?	Si (51,19) No (48,81)	El 51,19% de los estudiantes hace uso del equipo celular dentro de las aulas de clase mientras reciben la cátedra

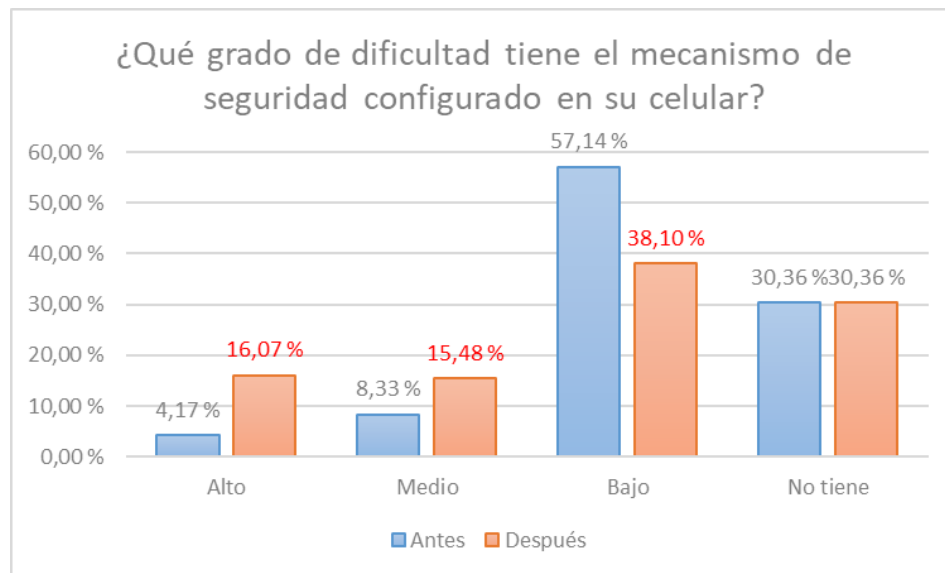
ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
35.	¿Con qué frecuencia hace uso del equipo móvil?	Siempre (0,00) Muchas veces (73,21) Con frecuencia (7,74) A veces (1,79) Alguna vez (0,00) Nunca (17,26)	El 73,21% de estudiantes están constantemente conectados y al tanto de lo que sucede a través de los equipos móviles
36.	¿Qué uso le da al equipo móvil?	Redes sociales (82,74) Fotografía (87,50) Consultas (82,74) Reproductor (82,74) Video (82,74) Radio (5,36) Juegos (82,74)	El 87,50% de los estudiantes hace uso del equipo móvil para toma de fotografías principalmente.
37.	¿Qué tipo de contenido consume en internet?	Humor (80,95) Sexual (73,81) Académico (82,74) Afectivo (82,74) Cultura Gral (78,57)	El 82,74% de estudiantes hacen uso del equipo móvil para desarrollar trabajos académicos y contenido afectivo.



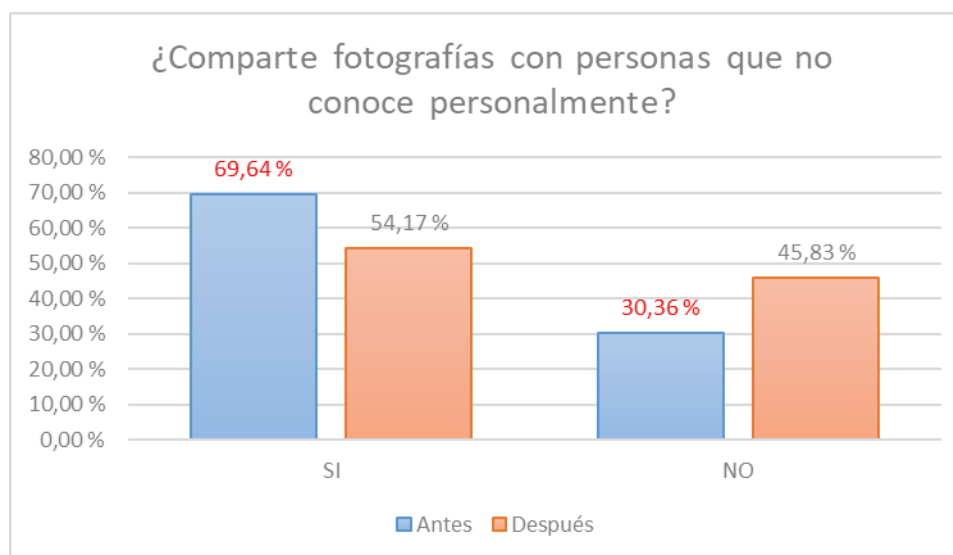
ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
38.	¿Qué red social consulta con más frecuencia con su equipo celular?	Facebook (63,69) Twitter (16,67) Google + (2,38) No (17,26)	El 63,69% de los estudiantes hacen uso de la red social Facebook para interactuar con otras personas.
39.	¿Instala software por fuera de la Play store, y App Store?	Si (35,12) No (64,88)	El 64,88% de los estudiantes están expuestos a software no autorizado por la empresa fabricante del sistema.
40.	¿Tiene implementado mecanismo de seguridad para acceder a su equipo?	Patrón (73,21) Huella (2,38) Facial (2,98) Números (1,19) No tiene (11,90) No aplica (8,33)	El 11,90% de estudiantes habilitaron algún mecanismo de seguridad para protección al acceso al equipo



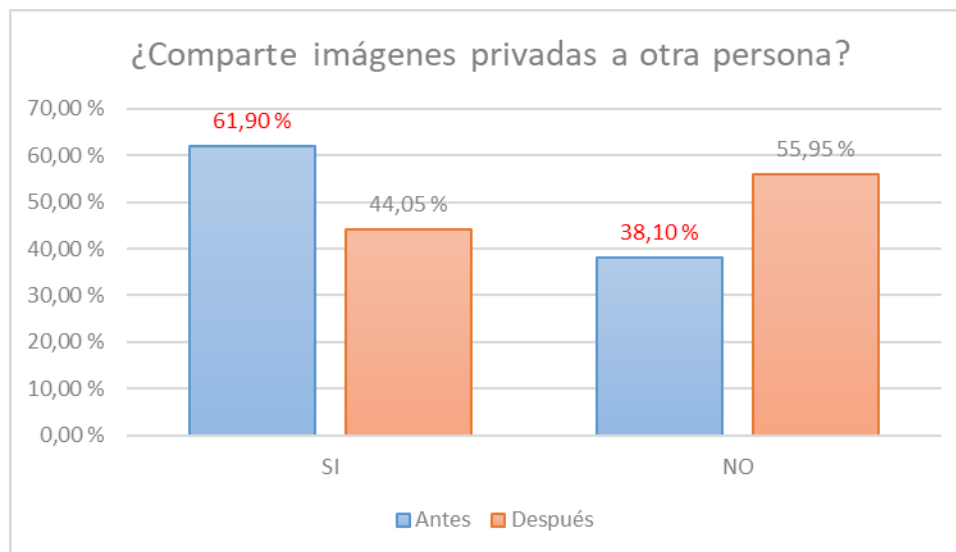
ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
41.	¿Qué grado de dificultad tiene el mecanismo de seguridad configurado en su celular?	Alto (16,07) Medio (15,48) Bajo (38,10) No tiene (30,36)	El 38,10% de estudiantes mejoró su patrón de seguridad.



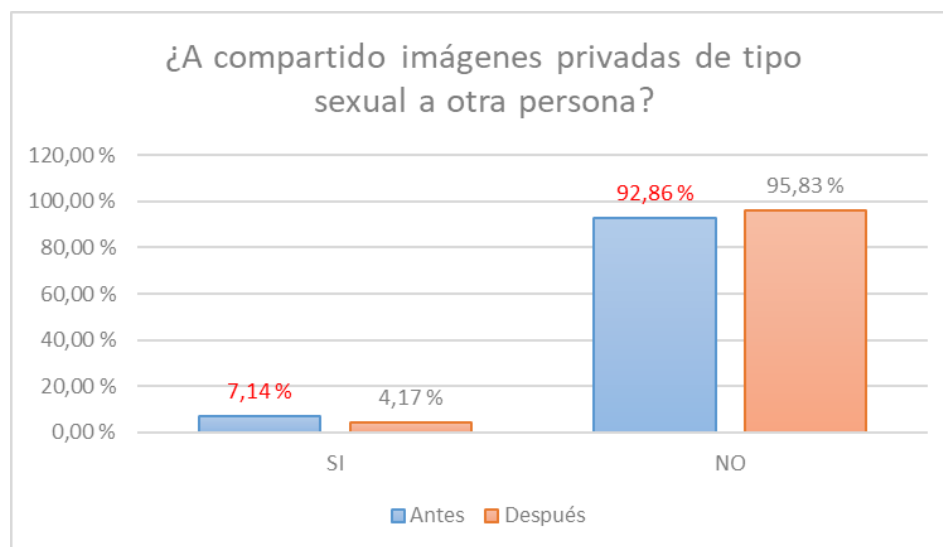
42.	¿Comparte fotografías con personas que no conoce personalmente?	Si (69,64) No (30,36)	El 69,64% de estudiantes están expuestos a ser víctimas de delitos por parte de personas desconocidas.
-----	---	--------------------------	--



ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
43.	¿Comparte imágenes privadas a otra persona?	Si (61,90) No (38,10)	El 61,90% de los estudiantes están expuestos a delitos como extorsión, abuso, pornografía al compartir imágenes de contenido privado



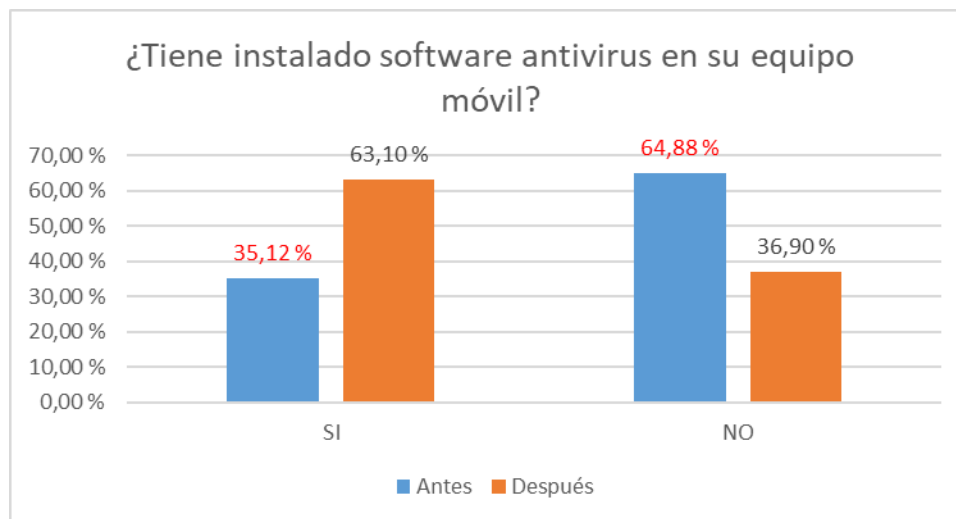
44.	¿A compartido imágenes privadas de tipo sexual a otra persona?	Si (7,14) No (92,86)	El 7,14% de los estudiantes están expuestos a delitos como explotación sexual, abuso, pornografía, al exponer imágenes de contenido privado
-----	--	-------------------------	---



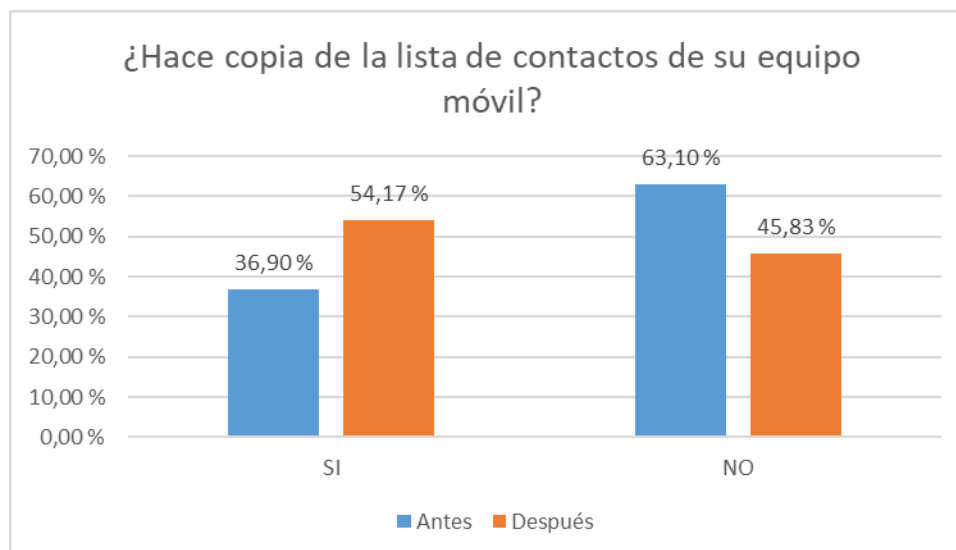


ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS																					
45.	¿Qué tan importante le resulta saber, lo que hagan otros con la información compartida de su parte?	Mucho (1,79) Algo (0,00) Poco (70,24) Nada (0,00) No lo había pensado (10,71) No (17,26)	Un 70,24% de los estudiantes están expuestos a delitos contra su persona debido a la poca importancia que le da al contenido que comparte, sin estar al tanto de las posibles consecuencias que se puedan presentar																					
<div><p>¿Qué tan importante le resulta saber, lo que hagan otros con la información compartida de su parte?</p><p>The bar chart displays the percentage of students who consider it important to know what others do with their shared information. The Y-axis represents the percentage from 0,00% to 80,00%. The X-axis lists the response categories: Mucho, Algo, Poco, Nada, No lo había pensado, and No. The legend indicates that blue bars represent 'Antes' (Before) and orange bars represent 'Después' (After). The data is as follows:</p><table><thead><tr><th>Respuesta</th><th>Antes (%)</th><th>Después (%)</th></tr></thead><tbody><tr><td>Mucho</td><td>1,79%</td><td>0,00%</td></tr><tr><td>Algo</td><td>0,00%</td><td>47,02%</td></tr><tr><td>Poco</td><td>32,14%</td><td>70,24%</td></tr><tr><td>Nada</td><td>0,00%</td><td>0,00%</td></tr><tr><td>No lo había pensado</td><td>10,71%</td><td>1,79%</td></tr><tr><td>No</td><td>17,26%</td><td>17,26%</td></tr></tbody></table></div>				Respuesta	Antes (%)	Después (%)	Mucho	1,79%	0,00%	Algo	0,00%	47,02%	Poco	32,14%	70,24%	Nada	0,00%	0,00%	No lo había pensado	10,71%	1,79%	No	17,26%	17,26%
Respuesta	Antes (%)	Después (%)																						
Mucho	1,79%	0,00%																						
Algo	0,00%	47,02%																						
Poco	32,14%	70,24%																						
Nada	0,00%	0,00%																						
No lo había pensado	10,71%	1,79%																						
No	17,26%	17,26%																						
46.	¿Su equipo celular ha sido infectado por virus?	Si (35,12) No (64,88)	El 35,12% de los estudiantes han sido afectados por infección de su equipo móvil que puede generar pérdida o robo de la información alojada en el equipo móvil																					

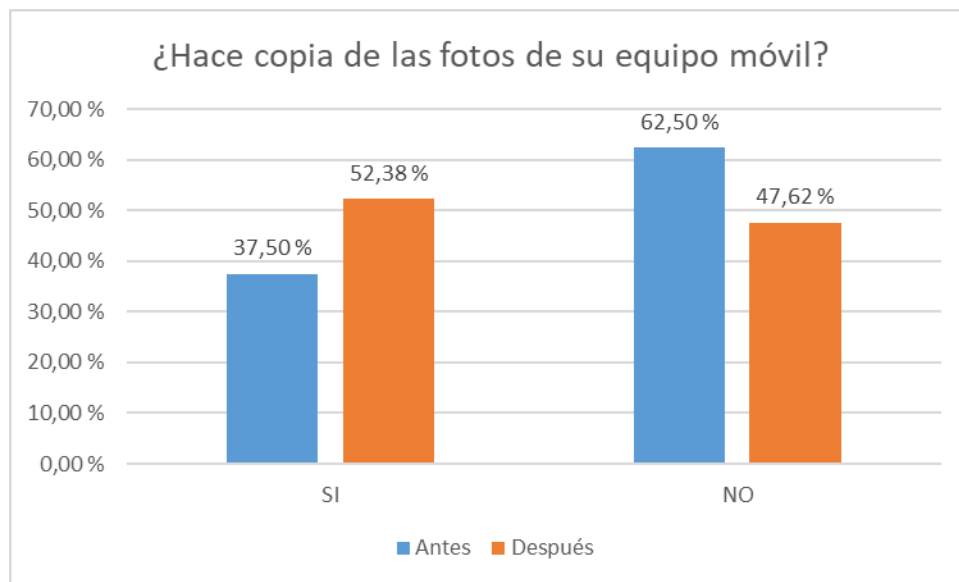
ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
47.	¿Tiene instalado software antivirus en su equipo móvil?	Si (35,12) No (64,88)	El 64,88% de los estudiantes no hace uso de un sistema de protección ante ataques de virus en el equipo móvil



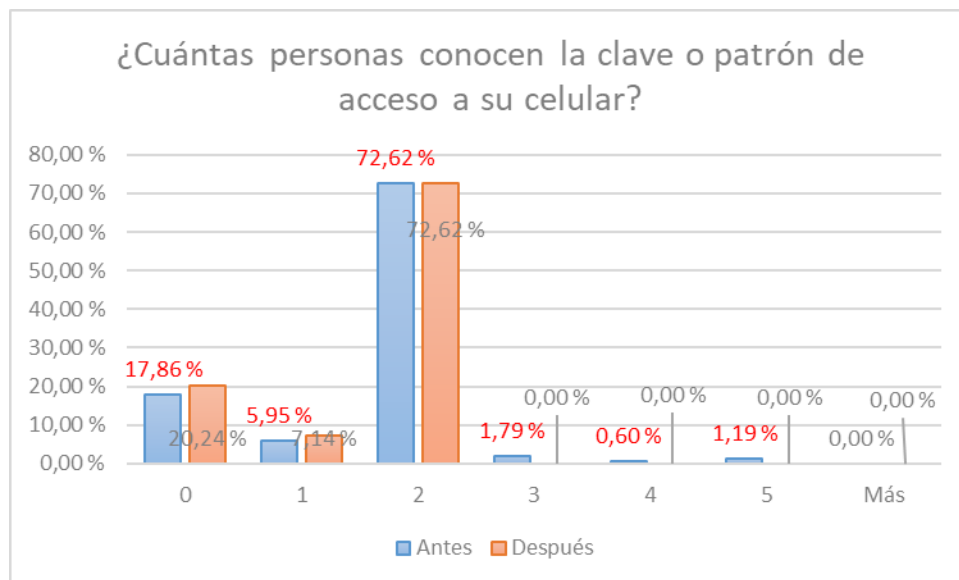
48.	¿Hace copia de la lista de contactos de su equipo móvil?	Si (36,90) No (63,10)	El 63,10% de los estudiantes están expuestos a pérdida o daño de los contactos de su dispositivo móvil.
-----	--	--------------------------	---



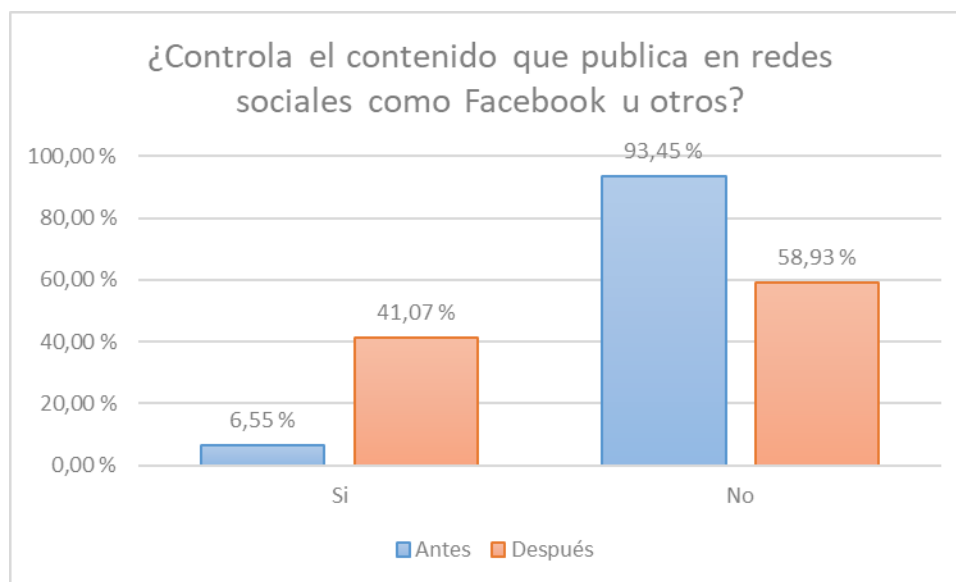
ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
49.	¿Hace copia de las fotos de su equipo móvil?	Si (37,50) No (62,50)	El 62,50% de los estudiantes están expuestos a pérdida o daño del contenido fotográfico de su dispositivo móvil.



ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
50.	¿Cuántas personas conocen la clave o patrón de acceso a su celular?	Cero (17,86) Una (5,95) Dos (72,62) Tres (1,79) Cuatro (0,60) Cinco (1,19) O Más (0,00)	El 72,62% de los estudiantes manifiestan compartir el mecanismo de acceso con dos personas adicionales, mientras que solo el 17,86% consideran una mayor privacidad en el uso de su dispositivo



ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
51.	¿Controla el contenido que publica en redes sociales como Facebook u otros?	Si (6,55) No (93,45)	El 93,45% de los estudiantes no está al tanto de los incidentes que pueden generarse al no controlar el público que sigue su perfil en las diferentes redes sociales, exponiéndose a delitos por parte de terceros.



ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS									
52.	¿Utiliza para conectarse a Internet redes públicas abiertas?	Si (76,19) No (23,81)	El 76,19% de los estudiantes están expuestos a robo, daño o espionaje de la información que fluye a través de los puntos de acceso públicos a internet									
<div><p>¿Utiliza para conectarse a Internet redes públicas abiertas?</p><table><thead><tr><th>Respuesta</th><th>Antes (%)</th><th>Después (%)</th></tr></thead><tbody><tr><td>Si</td><td>76,19</td><td>58,33</td></tr><tr><td>No</td><td>23,81</td><td>41,67</td></tr></tbody></table></div>				Respuesta	Antes (%)	Después (%)	Si	76,19	58,33	No	23,81	41,67
Respuesta	Antes (%)	Después (%)										
Si	76,19	58,33										
No	23,81	41,67										
53.	¿Le han pedido algún tipo de retribución o pago a cambio de no publicar o difundir información personal?	Si (4,76) No (95,24)	El 4,76% de los estudiantes han sido víctimas de algún tipo de delito generado por la información que publica de manera personal en las redes sociales o a través de aplicaciones del equipo móvil									
54.	¿Tiene alguna observación?	Si (2,98) No (97,02)	El 2,98% de los estudiantes manifiesta haber sido víctima de matoneo a raíz de información publicada a través de diferentes aplicaciones									

Fuente. Inédita

Luego de implementada la herramienta definida para disminuir los resultados obtenidos en la primera encuesta mediante charlas sobre seguridad informática, se realizó nuevamente el sondeo a través de la aplicación de la misma encuesta (Ver Tabla 2) para determinar una posible variación en los resultados inicialmente obtenido, obtenido como resultado los siguientes valores.

Tabla 2. Tabulación final encuesta aplicada

ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
28.	¿Cuenta con teléfono móvil?	Si (87,50) No (12,50)	Se mantuvo el número de equipos por estudiante durante el estudio.
29.	¿Qué tipo de teléfono móvil tiene?	Básico (4,76) Smartphone (79,17) Tablet con Simcard (3,57) No (12,50)	Se mantuvo la distribución de equipos por estudiante durante el estudio.
30.	¿Instala las actualizaciones disponibles del equipo celular (App y sistema operativo)?	Si ( <b>55,36</b> ) No ( <b>44,64</b> )	Se evidencia un cambio favorable sobre el "Si" de un <b>45,24%</b> con relación a la primera encuesta (10,12%) donde el estudiante se concientiza de la importancia de las actualizaciones de seguridad de sus equipos móviles.
31.	¿Tiene conexión a Internet constante?	Wifi (22,62) Plan (63,10) No (14,29)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
32.	¿Cuenta con plan de datos?	Prepago (31,55) Postpago (49,40) No (19,05)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
33.	¿Cuenta con plan de voz?	Prepago (32,74) Postpago (50,00) No (17,26)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
34.	¿Utiliza el equipo dentro del salón mientras está en clases?	Si (51,19) No (48,81)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
35.	¿Con qué frecuencia hace uso del equipo móvil?	Siempre (0,00) Muchas veces (73,21) Con frecuencia (7,74) A veces (1,79) Alguna vez (0,00) Nunca (17,26)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
36.	¿Qué uso le da al equipo móvil?	Redes sociales (82,74) Fotografía (87,50) Consultas (82,74) Reproductor (82,74) Video (82,74) Radio (5,36) Juegos (82,74)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
37.	¿Qué tipo de contenido consume en internet?	Humor (80,95) Sexual ( <b>57,74</b> ) Académico (82,74) Afectivo (82,74) Cultura Gral (78,57)	Se presenta una disminución del <b>16,07%</b> en cuanto al consumo de contenido sexual a través de internet con relación a la primera encuesta (73,81%) aplicada. Que se traduce en una disminución de la exposición del equipo móvil a infecciones o robo de información generadas por este tipo de sitios web
38.	¿Qué red social consulta con más frecuencia con su equipo celular?	Facebook (63,69) Twitter (16,67) Google + (2,38) No (17,26)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
39.	¿Instala software por fuera de la Play store, y App Store?	Si (35,12) No (64,88)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.

ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
40.	¿Tiene implementado mecanismo de seguridad para acceder a su equipo?	Patrón <b>(73,21)</b> Huella (2,38) Facial <b>(2,98)</b> Números (1,19) No tiene <b>(11,90)</b> No aplica (8,33)	Se evidencia una mejoría en la implementación de mecanismos de seguridad en un <b>8,33%</b> en el uso del mecanismo de acceso de "Patrón" frente al (64,88%) que tenía inicialmente, así como un aumento del <b>1,79%</b> frente al (1,19%) en el uso de reconocimiento facial.
41.	¿Qué grado de dificultad tiene el mecanismo de seguridad configurado en su celular?	Alto <b>(16,07)</b> Medio <b>(15,48)</b> Bajo <b>(38,10)</b> No tiene (30,36)	Se evidencia una mejora en el grado de dificultad en el mecanismo de seguridad que tenían los estudiantes del <b>11,90%</b> con relación al (4,17%) del nivel "Alto", y un <b>7,14%</b> del nivel "medio" con relación al (8,33%) que tenía inicialmente.
42.	¿Comparte fotografías con personas que no conoce personalmente?	Si <b>(54,17)</b> No <b>(45,83)</b>	Se evidencia una mejoría en la disminución de la práctica de compartir contenido con personas desconocidas en un <b>15,48%</b> con relación al "Si" en un (69,64%)
43.	¿Comparte imágenes privadas a otra persona?	Si <b>(44,05)</b> No <b>(55,95)</b>	Se evidencia una mejoría en la disminución de la práctica de compartir contenido privado con personas en un <b>17,86%</b> con relación al "Si" en un (61,90%)
44.	¿A compartido imágenes privadas de tipo sexual a otra persona?	Si <b>(4,17)</b> No <b>(95,83)</b>	Se evidencia una mejoría en la disminución de la práctica de compartir contenido de tipo sexual en un <b>2,98%</b> con relación al "Si" en un (7,14%)
45.	¿Qué tan importante le resulta saber, lo que hagan otros con la información compartida de su parte?	Mucho (1,79) Algo <b>(47,02)</b> Poco <b>(32,14)</b> Nada (0,00) No lo había pensado <b>(1,79)</b> No (17,26)	Se logra un cambio en la percepción de los estudiantes del <b>47,02%</b> que consideran en "Algo" la seguridad de su información que comparte frente al (0,00%) inicialmente reportado.
46.	¿Su equipo celular ha sido infectado por virus?	Si (35,12) No (64,88)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
47.	¿Tiene instalado software antivirus en su equipo móvil?	Si <b>(63,10)</b> No <b>(36,90)</b>	Mejora la protección del equipo móvil en un <b>27,98%</b> a partir del (35,12%) reportado inicialmente
48.	¿Hace copia de la lista de contactos de su equipo móvil?	Si <b>(54,17)</b> No <b>(45,83)</b>	Mejora la protección de los datos ante la pérdida de los contactos en un <b>17,26%</b> a partir de los (36,90%) reportados inicialmente.
49.	¿Hace copia de las fotos de su equipo móvil?	Si <b>(52,38)</b> No <b>(47,62)</b>	Se evidencia una mejoría en la protección ante pérdida o daño de contenido fotográfico del estudiante en un <b>14,88%</b> a partir del (37,50%) reportado inicialmente
50.	¿Cuántas personas conocen la clave o patrón de acceso a su celular?	Cero <b>(20,24)</b> Una <b>(7,14)</b> Dos (72,62) Tres <b>(0,00)</b>	Se evidencia un cambio de conciencia entre los estudiantes reduciendo el número de personas que pueden entrar a sus equipos



ITEM	PREGUNTA	RESPUESTAS (100%)	ANÁLISIS
		Cuatro (0,00) Cinco (0,00) O Más (0,00)	móviles limitando a máximo 2 personas. Para ello incrementan en un <b>2,38%</b> la limitación a <i>"solo un usuario, es quien conoce el mecanismo de acceso"</i> frente al (17,86%) inicialmente reportado, y en un <b>1,19%</b> al número de personas adicionales que conoce el mecanismo de acceso frente al (5,95%) inicialmente reportado
51.	¿Controla el contenido que publica en redes sociales como Facebook u otros?	Si (41,07) No (58,93)	Se evidencia un cambio favorable de percepción de un <b>34,52%</b> en el control del contenido publicado frente al (93,45%) de estudiante que NO lo hacían.
52.	¿Utiliza para conectarse a Internet redes públicas abiertas?	Si (58,33) No (41,67)	Se evidencia una disminución del <b>17,86%</b> en las conexiones a redes públicas frente al (23,81%) inicialmente reportado
53.	¿Le han pedido algún tipo de retribución o pago a cambio de no publicar o difundir información personal?	Si (4,76) No (95,24)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.
54.	¿Tiene alguna observación?	Si (2,98) No (97,02)	Se mantuvo el porcentaje de respuesta por estudiante durante el estudio.

Fuente. Inédita

## CONCLUSIONES

Luego de implementadas las herramientas establecidas para el desarrollo del presente proyecto se llega a las siguientes conclusiones de acuerdo con la muestra analizada:

- A pesar de que un número considerable de estudiantes pertenecen al estrato socio-económico 2, la capacidad de adquisición de equipos móviles de comunicación con capacidad de conexión a internet y redes sociales es “Alta”, por lo que se deduce que la necesidad de estar conectado a la Internet y sus servicios no depende directamente de esta variable.
- El estudio indica, que los estudiantes gran parte del tiempo suelen hacer uso de sus equipos móviles sin que sea una limitante la jornada estudiantil. Lo que se puede traducir en un mal hábito y desarrollo de malas prácticas que podrían disminuir el rendimiento académico de los estudiantes.
- A pesar de que los dispositivos móviles son una herramienta para obtener conocimiento, gran parte de los encuestados utilizan este medio para interrelacionarse con otros, a través de conversaciones y publicaciones de material fotográfico que expone el nivel de seguridad de los encuestados.
- El amplio uso de las redes sociales, abre la posibilidad de que terceros obtengan bastante información sobre hábitos, gustos, tendencias, familias y localizaciones de los integrantes de la muestra.
- Los estudiantes se les concientiza sobre la implicación que puede traer la distribución y alcance incontrolado de material fotográfico expuesto en la Internet.
- Se logra concientizar gran parte de la población encuestada, en la adopción y mejora de las prácticas de seguridad que permitan prevenir incidentes y delitos contra su persona o la de su círculo social/familiar.
- Los estudiantes de la muestra, son conscientes de la importancia y beneficios que les resulta el mantener sus equipos actualizados y con software de protección como antivirus, que les ayuda a proteger sus datos personales ante intereses de terceros.
- Se socializa entre la población, los canales de comunicación disponibles en caso de ser víctimas de delitos informáticos como son: sitio web de la policía ([https://adenunciar.policia.gov.co/adenunciar/frm\\_denuncia\\_di.aspx](https://adenunciar.policia.gov.co/adenunciar/frm_denuncia_di.aspx)), Centro Cibernético policial (<https://caivirtual.policia.gov.co/>) y línea de atención telefónica 123. Adicionalmente, se comparte enlaces sobre guías de seguridad generadas por la policía y el centro informático ([https://caivirtual.policia.gov.co/sites/default/files/guia\\_facebook.pdf](https://caivirtual.policia.gov.co/sites/default/files/guia_facebook.pdf) y [https://caivirtual.policia.gov.co/sites/default/files/guia\\_whatsapp.pdf](https://caivirtual.policia.gov.co/sites/default/files/guia_whatsapp.pdf))

## RECOMENDACIONES

- Realizar estudio, sobre el impacto que tiene el uso excesivo de equipos móviles en el desarrollo social, psicológico, afectivo, escolar, entre otros.
- Se debería, en aras de proteger la salud mental y social de los estudiantes, implementar controles y/o limitaciones más eficientes en el uso de los equipos móviles dentro de los ambientes escolares, con el objetivo de tengan mayor concentración sobre el conocimiento impartido en clase.
- Realizar estudio sobre tendencia de adquisición de equipos móviles en las diferentes edades de los jóvenes.
- Continuar con actividades de divulgación y concientización a través de charlas e info-guías, sobre temas de seguridad informática y protección de datos personales, entre los diferentes grupos estudiantiles de la Institución Educativa Catumare.

## DIFICULTADES

- A pesar de que se realice, difusión y concientización de la población en temas de seguridad informática, son muchos los estudiantes que pasan por alto la información suministrada exponiéndose a convertirse en víctimas de delitos informáticos.
- La falta de disposición de algunos pocos docentes, para disponer de sus horas de cátedra.
- A nivel técnico, se presentó una gran dificultad a la hora de plantear tanto las preguntas de la encuesta, como la dirección en la cual obtener los resultados luego de la tabulación de las respuestas.

BELKYN B RODRIGUEZ LEÓN  
Ingeniero de sistemas  
UNAD Acacias  
Diciembre 2018